



AUTOVIEW[®] 3008/3016
Installer/User Guide



USA Notification

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japanese Notification

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Korean Notification

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.

Safety and EMC Approvals and Markings

UL, FCC, cUL, ICES-003, CE, VCCI, MIC, C-Tick, GOST





AutoView[®] 3008/3016 Switch Installer/User Guide

Avocent, the Avocent logo, The Power of Being There, AutoView, Dambrackas Video Compression and OSCAR are registered trademarks of Avocent Corporation or its affiliates in the U.S. and other countries. All other marks are the property of their respective owners.

© 2010 Avocent Corporation. 590-920-501C

**Instructions**

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

**Dangerous Voltage**

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

**Power On**

This symbol indicates the principal on/off switch is in the on position.

**Power Off**

This symbol indicates the principal on/off switch is in the off position.

**Protective Grounding Terminal**

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

List of Figures	vii
List of Tables	ix
Chapter 1: Product Overview	1
<i>Features and Benefits</i>	<i>1</i>
<i>Reduce cable bulk</i>	<i>1</i>
<i>Access the AutoView 3008/3016 switch via a standard TCP/IP network</i>	<i>2</i>
Chapter 2: Installation	3
<i>AutoView 3008/3016 Switch Connectivity</i>	<i>3</i>
<i>Installation Overview</i>	<i>3</i>
<i>Getting started</i>	<i>5</i>
<i>Setting up your network</i>	<i>5</i>
<i>Rack Mounting an AutoView 3008/3016 Switch</i>	<i>6</i>
<i>Rack mounting safety considerations</i>	<i>6</i>
<i>Connecting the AutoView 3008/3016 Switch Hardware</i>	<i>6</i>
<i>Adjusting Mouse Settings on Target Devices</i>	<i>8</i>
<i>Connecting to the OBWI Through a Firewall</i>	<i>8</i>
<i>Verifying the Connections</i>	<i>10</i>
<i>AutoView 3008/3016 switch</i>	<i>10</i>
<i>IQ and serial IQ modules</i>	<i>10</i>
<i>Cascading AutoView Switches</i>	<i>10</i>
Chapter 3: Local Port Operation	13
<i>Basic Operations</i>	<i>13</i>
<i>Main Dialog Box Functions</i>	<i>13</i>
<i>Viewing and selecting ports and servers</i>	<i>14</i>
<i>Selecting a target device</i>	<i>14</i>
<i>Soft switching</i>	<i>15</i>
<i>Viewing the status of your AutoView 3008/3016 switching system</i>	<i>15</i>
<i>Navigating the OSCAR interface</i>	<i>16</i>
<i>Setup Dialog Box Functions</i>	<i>17</i>
<i>Changing the display behavior</i>	<i>18</i>

<i>Controlling the status flag</i>	19
<i>Setting the keyboard country code</i>	21
<i>Configuring network settings</i>	22
<i>Assigning device types</i>	22
<i>Assigning target device names</i>	24
Commands Dialog Box Functions	25
<i>Selecting target devices for Scan mode</i>	26
<i>Enabling or disabling Scan mode</i>	27
<i>Viewing and disconnecting user connections</i>	28
<i>Displaying version information and upgrading firmware</i>	29
<i>Resetting the PS/2 keyboard and mouse on a target device or local port</i>	32
Chapter 4: Web Interface Operations	35
<i>AutoView 3008/3016 Switch OBWI</i>	35
<i>Viewing and Selecting Ports and Servers</i>	36
<i>The AutoView 3008/3016 Explorer Window</i>	36
<i>Launching a KVM Session</i>	38
<i>Viewing and terminating user sessions</i>	38
<i>Session sharing options</i>	39
<i>Managing the AutoView 3008/3016 switch OBWI</i>	41
<i>Managing users</i>	41
<i>Access levels</i>	41
<i>Managing Device Properties</i>	45
<i>Viewing and changing appliance configuration information</i>	45
<i>Enabling Network Time Protocol (NTP) functionality</i>	47
<i>Configuring an Override Admin Account</i>	47
<i>Enabling and configuring SNMP</i>	47
<i>Viewing and resynchronizing server connections</i>	49
<i>Modifying a server name</i>	50
<i>Viewing the IQ modules and IACs</i>	51
<i>Viewing and configuring cascaded switch connections</i>	51
<i>Viewing version information</i>	52
<i>Upgrading firmware</i>	54
<i>Rebooting the switch</i>	56

<i>Managing AutoView switch configuration files</i>	56
<i>Managing user databases</i>	58
<i>Configuring LDAP</i>	60
<i>LDAP Overview parameters</i>	60
<i>LDAP Search parameters</i>	61
<i>LDAP Query parameters</i>	61
<i>Appliance and Server Query Modes</i>	62
<i>Setting up Active Directory for performing queries</i>	63
<i>Installing a Web Certificate</i>	64
Chapter 5: The Video Viewer	67
<i>The Video Viewer Window</i>	67
<i>Video Viewer Window Features</i>	67
<i>Changing the toolbar</i>	69
<i>Setting the window size</i>	69
<i>Adjusting the view</i>	70
<i>Adjusting color depth</i>	71
<i>Additional video adjustment</i>	71
<i>Target video settings</i>	73
<i>Contrast and brightness</i>	73
<i>Detection thresholds</i>	73
<i>Block Noise Threshold and Pixel Noise Threshold</i>	73
<i>Automatic video adjustment</i>	73
<i>Refresh Image</i>	74
<i>Video Test Pattern</i>	74
<i>Adjusting mouse options</i>	74
<i>Cursor type</i>	74
<i>Mouse scaling</i>	76
<i>Vendor-specific video settings</i>	77
<i>Mouse alignment and synchronization</i>	77
<i>Using Keyboard Pass-through</i>	77
<i>Using Macros</i>	78
<i>Saving the View</i>	78
<i>Closing a Video Viewer Window Session</i>	79
Chapter 6: Terminal Operations	81

<i>The Console Menu</i>	81
<i>Network Configuration</i>	81
<i>Other Console Main Menu Options</i>	82
<i>Firmware Management</i>	82
<i>Enable Debug Messages</i>	82
<i>Set/Change Password</i>	82
<i>Restore Factory Defaults</i>	82
<i>Reset Appliance</i>	82
<i>Set Web Interface Ports</i>	83
<i>Input Web Server Certificate</i>	83
<i>Exit</i>	83
Appendices	85
<i>Appendix A: Flash Upgrades</i>	85
<i>Appendix B: Using Serial IQ Modules</i>	87
<i>Appendix C: UTP Cabling</i>	91
<i>Appendix D: Technical Specifications</i>	93
<i>Appendix E: Sun Advanced Key Emulation</i>	95
<i>Appendix F: Technical Support</i>	97

LIST OF FIGURES

<i>Figure 1.1: Example Switch Configuration (AutoView 3016 Switch Shown)</i>	2
<i>Figure 2.1: Basic AutoView 3016 Switch Configuration</i>	4
<i>Figure 2.2: Typical AutoView 3008/3016 Switch Firewall Configuration</i>	9
<i>Figure 3.1: OSCAR Interface Main Dialog Box</i>	13
<i>Figure 3.2: OSCAR Interface Setup Dialog Box</i>	18
<i>Figure 3.3: OSCAR Interface Menu Dialog Box</i>	18
<i>Figure 3.4: OSCAR Interface Flag Dialog Box</i>	20
<i>Figure 3.5: Position Flag</i>	20
<i>Figure 3.6: OSCAR Interface Keyboard Dialog Box</i>	21
<i>Figure 3.7: OSCAR Interface Network Dialog Box</i>	22
<i>Figure 3.8: OSCAR Interface Devices Dialog Box</i>	23
<i>Figure 3.9: OSCAR Interface Device Modify Dialog Box</i>	23
<i>Figure 3.10: OSCAR Interface Names Dialog Box</i>	24
<i>Figure 3.11: OSCAR Interface Name Modify Dialog Box</i>	25
<i>Figure 3.12: OSCAR Interface Commands Dialog Box</i>	26
<i>Figure 3.13: Scan Dialog Box</i>	27
<i>Figure 3.14: OSCAR Interface User Status Dialog Box</i>	28
<i>Figure 3.15: OSCAR Interface Disconnect Dialog Box</i>	29
<i>Figure 3.16: OSCAR Interface Version Dialog Box</i>	30
<i>Figure 3.17: AVRIQ Selection Dialog Box</i>	30
<i>Figure 3.18: AVRIQ Version Dialog Box</i>	31
<i>Figure 3.19: AVRIQ Status Dialog Box</i>	32
<i>Figure 4.1: Avocent AutoView 3016 Explorer Window</i>	37
<i>Figure 4.2: Disconnect Session Status Window</i>	39
<i>Figure 4.3: Users Window</i>	43
<i>Figure 4.4: Add/Modify User Window</i>	43
<i>Figure 4.5: Sessions Window</i>	46
<i>Figure 4.6: SNMP Window</i>	48
<i>Figure 4.7: Traps Window</i>	49
<i>Figure 4.8: Servers Window</i>	50
<i>Figure 4.9: Modify Server Name Window</i>	51

<i>Figure 4.10: Versions Window</i>	52
<i>Figure 4.11: AVRIQ Versions Window</i>	53
<i>Figure 4.12: Upgrade Appliance Firmware (TFTP Server) Window</i>	55
<i>Figure 4.13: Upgrade Appliance Firmware (File System) Window</i>	55
<i>Figure 4.14: Save Appliance Configuration Window (File System)</i>	57
<i>Figure 4.15: Save Appliance User Data Window (FTP Server)</i>	57
<i>Figure 4.16: Restore Appliance User Data (File System) Window</i>	59
<i>Figure 4.17: Restore Appliance User Data (FTP Server) Window</i>	59
<i>Figure 4.18: Install Web Server Certificate Window</i>	65
<i>Figure 5.1: Video Viewer Window (Normal Window Mode)</i>	68
<i>Figure 5.2: Manual Video Adjust Dialog Box</i>	72
<i>Figure 5.3: Video Viewer Window with Local and Remote Cursors Displayed</i>	75

LIST OF TABLES

<i>Table 1.1: Descriptions for Figure 1.1</i>	2
<i>Table 2.1: Descriptions for Figure 2.1</i>	5
<i>Table 2.2: TCP Ports and Functions for the AutoView 3008/3016 Switch</i>	8
<i>Table 2.3: Descriptions for Figure 2.2</i>	9
<i>Table 3.1: Main Dialog Box Functions</i>	13
<i>Table 3.2: OSCAR Interface Status Symbols</i>	15
<i>Table 3.3: OSCAR Interface Navigation Basics</i>	16
<i>Table 3.4: Setup Features to Configure the OSCAR Interface</i>	17
<i>Table 3.5: OSCAR Interface Status Flags</i>	19
<i>Table 3.6: Commands to Manage Routine Tasks for Your Target Devices</i>	25
<i>Table 4.1: OBWI Supported Operating Systems and Browsers</i>	35
<i>Table 4.2: Descriptions for Figure 4.1</i>	37
<i>Table 4.3: Session Sharing Definitions</i>	40
<i>Table 4.4: Allowed Operations by Access Level</i>	41
<i>Table 4.5: User Access Level Rights</i>	42
<i>Table 5.1: Descriptions for Figure 5.1</i>	68
<i>Table 5.2: Descriptions for Figure 5.2</i>	72
<i>Table 5.3: Descriptions for Figure 5.3</i>	75
<i>Table B.1: Serial IQ Module Pinouts</i>	90
<i>Table C.1: UTP Wiring Standards</i>	91
<i>Table D.1: AutoView 3008/3016 Switch Product Specifications</i>	93
<i>Table E.1: Sun Key Emulation</i>	95
<i>Table E.2: PS/2-to-USB Keyboard Mappings</i>	96

Product Overview

Features and Benefits

Avocent AutoView 3008/3016 switches combine analog and digital technology to provide flexible control of data center servers, and to facilitate the OA&M (operations, activation and maintenance) of remote branch offices where trained operators may be unavailable. The AutoView 3008/3016 switches provide users with a significant reduction of cable volume, secure remote access and flexible server management from anywhere at anytime.

The AutoView 3008/3016 KVM switch family has several options depending on the model:

- a rack mountable keyboard, video and mouse (KVM) switch, configurable for analog (local) or digital (remote) connectivity
- support for VGA, SVGA, SGA and SXGA video
- video resolutions up to 1600 x 1200 for local and remote users
- accessibility to target devices across 10/100 LAN port(s)
- cascading expansion; each AutoView switch supports up to 16 directly attached servers and can conveniently scale to support more

Reduce cable bulk

With server densities continually increasing, cable bulk remains a major concern for network administrators. The AutoView 3008/3016 switches significantly reduce KVM cable volume in the rack by utilizing the innovative IQ module and single, industry-standard Unshielded Twisted Pair (UTP) cabling or the Integrated Access Cable (IAC) cabling option. This allows a higher server density while providing greater airflow and cooling capacity.

NOTE: All references to IQ modules in this document use the AVRIQ module as a default, except where indicated differently. AutoView 3008/3016 switches support AVRIQ, DSRIQ, DSAVIQ and IAC modules.

The IQ and IAC modules are powered directly from the target device and provide Keep Alive functionality when the switch is not turned on. The serial IQ module is a DCE device that provides the primary interface between a serial device and an AutoView 3008/3016 switch. It provides VT100 terminal emulation, break suppression and port history in a compact, convenient module.

Access the AutoView 3008/3016 switch via a standard TCP/IP network

The Avocent AutoView 3008/3016 switches provide agentless remote control and access. No special software or drivers are required on the attached, or client, computers. The client connects to the AutoView 3008/3016 switch using an Internet browser.

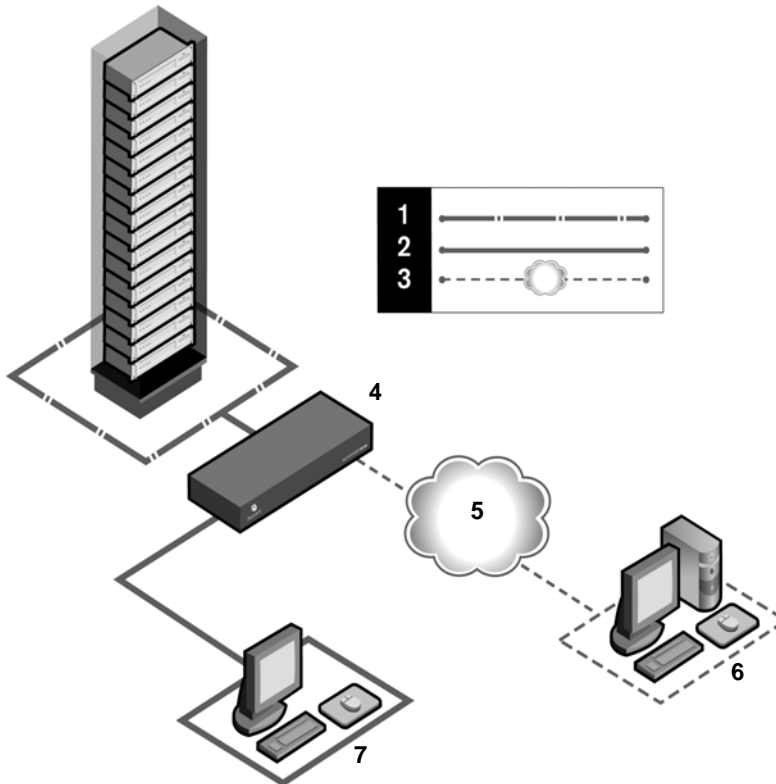


Figure 1.1: Example Switch Configuration (AutoView 3016 Switch Shown)

Table 1.1: Descriptions for Figure 1.1

Number	Description	Number	Description
1	UTP Connection	5	Network
2	KVM Connection to the Switch	6	Digital User (Computer with Internet Browser)
3	Remote IP Connection	7	Analog User (OSCAR® Graphical User Interface)
4	AutoView 3016 Switch		

AutoView 3008/3016 Switch Connectivity

The AutoView 3008/3016 switching system transmits keyboard, video and mouse (KVM) information between operators and target devices attached to the switch.

The AutoView 3008/3016 switch uses TCP/IP for communication over a network. Although 10BaseT Ethernet may be used, Avocent recommends a dedicated, switched 100BaseT network.

Installation Overview

The general procedure for setting up and installing an AutoView 3008/3016 switch is as follows:

- Unpack the switch and verify that all components are present and in good condition.
- Make all hardware connections between the power source, switch, target devices and the Ethernet.
- Turn on the power and verify that all connections are working.
- Configure the AutoView 3008/3016 switch's IP address using the OSCAR graphical user interface.
- Use the On-board Web Interface (OBWI) to configure the AutoView 3008/3016 switch.
- Make the appropriate mouse setting adjustments.

Figure 2.1 illustrates a basic configuration for the AutoView 3016 switch. Descriptions follow in Table 2.1.

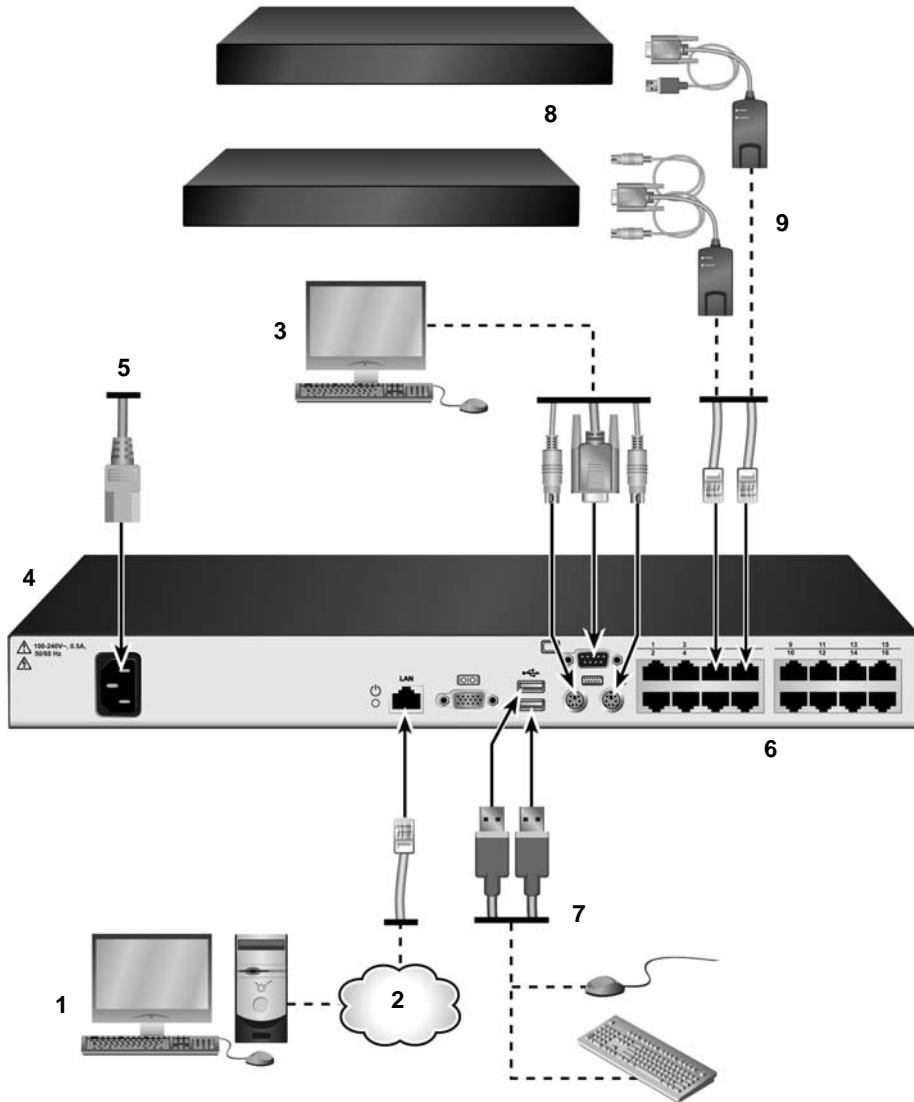


Figure 2.1: Basic AutoView 3016 Switch Configuration

Table 2.1: Descriptions for Figure 2.1

Number	Description	Number	Description
1	Digital User	6	Ports 1-16
2	Network	7	Local USB Connections
3	Analog User	8	Servers 1-16
4	AutoView 3016 Switch	9	IQ or IAC modules, PS/2, USB, Sun and serial adaptors are available
5	Power Cord		

Getting started

Before installing your AutoView 3008/3016 switch, refer to the following lists to ensure you have all items that shipped with the switch, as well as other items necessary for proper installation.

Supplied with the AutoView 3008/3016 switch

- Local country power cord
- Rack mounting brackets
- Rack Mounting Bracket Quick Installation Guide
- AutoView 3008/3016 Switch Quick Installation Guide
- One DB9 M/F serial cable

Additional items needed

- One IQ module per target server or serial IQ module per serial device. IAC cables can also be used.
- One UTP patch cable per IQ module (4-pair UTP, up to 30 meters)
- UTP patch cable(s) for network connectivity (4-pair UTP, up to 30 meters)

Setting up your network

The AutoView 3008/3016 switching system uses IP addresses to uniquely identify the switch and the target devices. The AutoView 3008/3016 switch family supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Avocent recommends that IP addresses be reserved for each switch and that they remain static while the switches are connected to the network.

Rack Mounting an AutoView 3008/3016 Switch

A rack mounting kit is supplied with each AutoView 3008/3016 switch. You may either place the AutoView 3008/3016 switch on the rack shelf or mount the switch directly into an Electronic Industries Alliance (EIA) standard rack.

AutoView 3008/3016 switches are rack mounted in a 1U configuration. The AutoView 3008/3016 switch family does not support a 0U configuration.

Rack mounting safety considerations

- **Rack Loading:** Overloading or uneven loading of racks may result in shelf or rack failure, causing damage to equipment and possible personal injury. Stabilize racks in a permanent location before loading begins. Mount components beginning at the bottom of the rack, then work to the top. Do not exceed your rack load rating.
- **Power Considerations:** Connect only to the power source specified on the unit. When multiple electrical components are installed in a rack, ensure that the total component power ratings do not exceed circuit capabilities. Overloaded power sources and extension cords present fire and shock hazards.
- **Elevated Ambient Temperature:** If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the switch.
- **Reduced Air Flow:** Install the equipment in the rack so that the amount of airflow required for safe operation of the equipment is not compromised.
- **Reliable Earthing:** Maintain reliable earthing of rack mounted equipment. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

To install the rack mounting bracket:

1. Remove the two rack mounting screws from each side of the AutoView 3008/3016 switch.
2. Place the rack mounting brackets next to the switch.
3. Insert the screws supplied with the rack mounting kit through the holes of the brackets and into the AutoView 3008/3016 switch. Tighten the screws securely.
4. Install the AutoView 3008/3016 switch into the rack using the method of the rack manufacturer.

Connecting the AutoView 3008/3016 Switch Hardware

To connect and turn on your AutoView 3008/3016 switch:

CAUTION: You must turn off all servers that will be part of your AutoView switching system. Wait until step 6 to turn on your AutoView switch.

1. Plug your monitor and either PS/2 or USB keyboard and mouse cables into the appropriately labeled ports on the AutoView switch.
2. Plug a compatible IQ or IAC module into the appropriate ports on the back of the target server.
3. Choose an available numbered port on the rear of your AutoView 3008/3016 switch. Plug the IAC cable or one end of a UTP patch cable (4-pair, up to 45 meters) into the selected port and plug the other end into the RJ-45 connector of the IQ module. Repeat this procedure for all servers that are to be connected to the AutoView 3008/3016 switch.

NOTE: When connecting a Sun IQ module, you must use a multi-sync monitor in the local port to accommodate Sun computers that support VGA or composite sync.

4. Plug a UTP patch cable from your Ethernet network into the LAN port on the back of your AutoView 3008/3016 switch. Network users will access the AutoView 3008/3016 switch through this port.
5. Locate the power cord that came with the AutoView 3008/3016 switch and plug the appropriate end into the power socket on the rear of the switch. Plug the other end into an appropriate AC wall outlet.

NOTE: To avoid potential video and/or keyboard problems when using Avocent products: If the building has 3-phase AC power, ensure that the computer and monitor are on the same phase. For best results, they should be on the same circuit.

WARNING: To reduce the risk of electric shock or damage to your equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
 - Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.
 - Disconnect the power from the switch by unplugging the power cord from either the electrical outlet or the appliance.
 - The AC inlet is the main power disconnect.
-

6. Turn on the AutoView switch and monitor, then turn on each target device. After about one minute, the switch completes initialization and displays the OSCAR graphical user interface Free tag on the local port monitor.
7. Depending on how you will access the switch, you can configure the network settings through the OSCAR interface On-Screen Display (OSD) or the On-Board Web Interface (OBWI).

To configure network settings via the OSCAR interface:

1. Press **Print Screen** to activate the OSCAR interface Main dialog box.
2. Click *Setup - Network* and enter the appropriate Network Speed, Transmission Mode and Network Configuration settings for your network.

To configure network settings via the OBWI:

1. Point your web browser to the default IP address **https://192.168.1.1** to access the switch.
2. Log in to the OBWI and click the *Configure* tab.

3. In the Appliance Configuration menu on the left, click *Appliance - Network* and enter the appropriate Network Speed, Transmission Mode and Network Configuration settings for your network.

To connect a serial IQ module to a serial device:

1. Attach the serial IQ module 9-pin serial connector to the serial port of the device to be connected to your AutoView 3008/3016 switch.
2. Attach one end of the UTP patch cable to the RJ-45 connector on the IQ module. Connect the other end of the UTP patch cable to the desired port on the back of your AutoView 3008/3016 switch.

NOTE: The serial IQ module is a DCE device and only supports VT100 terminal emulation.

3. Connect the power supply to the power connector on your serial IQ module. The cable expander can be used to turn on up to four serial IQ modules from a single power supply.
4. Connect the serial IQ module power supply to a grounded AC wall outlet. Turn on your serial device. See the *Using Serial IQ Modules* on page 87 for more information.

Adjusting Mouse Settings on Target Devices

Before a computer connected to the AutoView 3008/3016 switch can be used for remote user control, you must set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® operating systems, use the default PS/2 mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to “none” for all user accounts accessing a remote system through a KVM switch. Mouse acceleration must also be set to “none” on every remote system. Special cursors should not be used and cursor visibility options such as pointer trails, **Ctrl** key cursor location animations, cursor shadowing and cursor hiding, should also be turned off. For more information, see the Mouse and Pointer Settings Technical Bulletin available at www.avocent.com.

Connecting to the OBWI Through a Firewall

For AutoView 3008/3016 switch installations that use the OBWI for access, four ports must be opened in a firewall if outside access is desired.

Table 2.2: TCP Ports and Functions for the AutoView 3008/3016 Switch

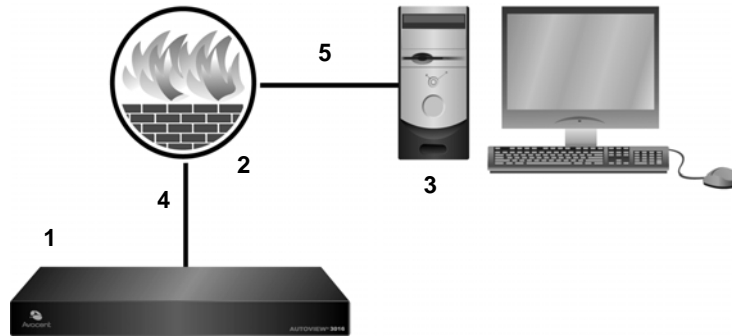
TCP Port Number	Function
80	Can be used for the initial downloading of the Video Viewer (for downloading the Java applet)
443	Can be used by the web browser interface for managing the AutoView 3008/3016 switch and launching KVM sessions

Table 2.2: TCP Ports and Functions for the AutoView 3008/3016 Switch (Continued)

TCP Port Number	Function
2068	Transmission of KVM session data (mouse & keyboard) or transmission of video for AutoView 3008/3016 switches
8192	Transmission of KVM session data (video) for AutoView 3008/3016 switches

NOTE: Ports 80 and 443 are configurable by the appliance administrator.

In a typical configuration, as shown in Figure 2.2, the user's computer is located outside of the firewall, and the AutoView 3008/3016 switch resides inside the firewall.

**Figure 2.2: Typical AutoView 3008/3016 Switch Firewall Configuration****Table 2.3: Descriptions for Figure 2.2**

Number	Description
1	AutoView 3016 Switch
2	Firewall
3	User's Computer
4	Firewall (Forwards HTTP Requests and KVM Traffic to the AutoView 3008/3016 Switch)
5	User (Browses to Firewall's External IP Address)

To configure the firewall:

To access the AutoView 3008/3016 switch from outside a firewall, configure your firewall to forward ports 80, 443, 2068 and 8192 from its external interface to the KVM switch through the firewall's internal interface. Consult the manual for your firewall for specific port forwarding instructions.

To connect to the AutoView 3008/3016 switch OBWI from outside the firewall:

Open a web browser and enter the external IP address of the firewall. The AutoView 3008/3016 Explorer window will open and prompt you to login.

Verifying the Connections

AutoView 3008/3016 switch

The rear panel of the AutoView 3008/3016 switch features LEDs indicating the Ethernet connection for LAN, as well as LEDs that indicate the target device status for each port.

Ethernet connection LEDs

- The green LED, labeled *Link*, illuminates when a valid connection to the network is established at the maximum supported rate and blinks when there is activity on the port.
- The amber LED illuminates when an Ethernet connection is communicating at a slower rate.
- If neither LED is illuminated, connection speed is at a rate of 10 Mbps.

IQ and serial IQ modules

Typically, IQ modules feature two green LEDs: a *POWER* LED and a *STATUS* LED.

- The *POWER* LED indicates that the attached module is turned on.
- The *STATUS* LED indicates that a valid selection has been made to an AutoView 3008/3016 switch.

The serial IQ module prevents a serial break from the attached device if the module loses power. However, a user can generate a serial break with the attached device by pressing **Alt-B** after accessing the Terminal Applications menu.

Cascading AutoView Switches

You can cascade other AutoView switch models to an AutoView 3008/3016 switch via a CAT 5 cable. In a cascaded system, an available target port on the AutoView 3008/3016 switch will connect to an AVRIQ-PS/2 module or ACI (Avocent Console Interface) port on each cascaded AutoView switch.

NOTE: In a cascaded configuration, the AutoView 3008/3016 switch must be at the top of the cascade.

To cascade multiple AutoView switches if your switch has an ACI port:

1. Using an appropriate length of CAT 5 cable, connect the ACI port on the cascaded switch to an available port on your 3008/3016 switch.
2. Repeat step 1 for all additional cascaded AutoView switches.

To cascade multiple AutoView switches if your switch does not have an ACI port:

1. Connect an AVRIQ-PS/2 module to the local peripheral ports on the cascaded switch.
2. Using an appropriate length of CAT 5 cable, connect the AVRIQ-PS/2 module from step 1 to an available port on your 3008/3016 switch.
3. Repeat steps 1 and 2 for all additional cascaded AutoView switches.

NOTE: The system will automatically “merge” the two switches together as one. All servers connected to the cascaded AutoView switch will display on the main AutoView switch server list in the OSCAR interface.

Local Port Operation

AutoView 3008/3016 switch users can access attached devices via the OSCAR interface OSD or the OBWI. For information on the OBWI, see Chapter 4.

Basic Operations

Main Dialog Box Functions

To access the OSCAR interface Main dialog box:

Press **Print Screen** to launch the OSCAR interface. The Main dialog box will appear.

NOTE: If OSCAR Password has been enabled, you will be prompted to enter a password before you can launch the OSCAR interface.

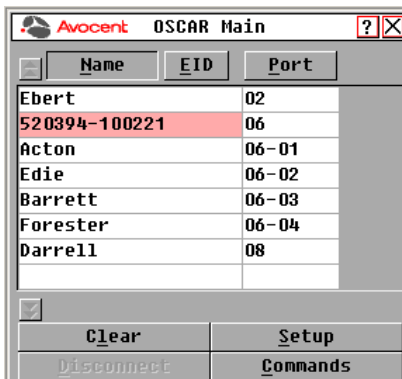


Figure 3.1: OSCAR Interface Main Dialog Box

Table 3.1: Main Dialog Box Functions

Button	Function
Clear	Clear all offline IQ modules.
Disconnect	Disconnect the KVM session.

Table 3.1: Main Dialog Box Functions (Continued)

Button	Function
Setup	Access the Setup dialog box and configure the OSCAR interface.
Commands	Access the Commands dialog box.
Name	Name of server.
EID	Unique Electronic ID in a module.
Port	The port to which a target device is connected.

Viewing and selecting ports and servers

Use the Main dialog box to view, configure and control target devices in the AutoView 3008/3016 switching system. You may view the target devices by name, port or by the unique Electronic ID (EID) embedded in each IQ module. You will see an OSCAR interface-generated port list by default when you first launch the OSCAR interface.

The Port column indicates the port to which a target device is connected.

Selecting a target device

Use the Main dialog box to select a target device. When you select a target device, the AutoView 3008/3016 switch reconfigures the local keyboard and mouse to the settings for the selected target device.

To select a target device:

Double-click the target device name, EID or port number.

-or-

If the display order of your list is by port (the *Port* button is depressed), type the port number and press **Enter**.

-or-

If the display order of your list is by name or EID (the *Name* or *EID* button is depressed), type the first few letters of the name of the target device or the EID number to establish it as unique and press **Enter**.

To select the previous target device:

Press **Print Screen** and then **Backspace**. This key combination toggles you between the previous and current connections.

To disconnect from a target device:

Press **Print Screen** and then **Alt+0** (zero). This leaves the user in a free state, with no target device selected. The status flag on your desktop displays *Free*.

Soft switching

Soft switching is the ability to switch target devices using a hotkey sequence. You can soft switch to a target device by pressing **Print Screen** and then, depending on the method you've selected, typing the first few characters of its name or number. If you have set a Screen Delay Time for the OSCAR interface and you press the key sequences before that time has elapsed, the OSCAR interface will not display.

To soft switch to a target device:








Press **Print Screen** and type the port number the first few letters of the name of the target device to establish it as unique and press **Enter**.

To switch back to the previous target device, press **Print Screen** then **Backspace**.

Viewing the status of your AutoView 3008/3016 switching system

The status of target devices in your system is indicated in the far right columns of the Main dialog box. The following table describes the status symbols.

Table 3.2: OSCAR Interface Status Symbols

Symbol	Description
	(green circle) Server connected, turned on and the IQ module is online.
	Connected target device is turned off or is not operating properly, and the IQ module is offline.
	Connected switch is online.
	Connected switch is offline or not operating properly.
	(yellow circle) The designated IQ module is being upgraded. When this symbol displays, do not cycle power to the AutoView 3008/3016 switch or connected target devices and do not disconnect IQ modules. Doing so may render the module permanently inoperable and require the IQ module to be returned to the factory for repair.
	(green letter) IQ module is being accessed by the indicated user channel.
	(black letter) IQ module is blocked by the indicated user channel.

Navigating the OSCAR interface

This table describes how to navigate the OSCAR interface using the keyboard and mouse.

Table 3.3: OSCAR Interface Navigation Basics

Keystroke	Function
<Print Screen>, Ctrl-Ctrl, Shift-Shift and/or Alt-Alt	OSCAR interface activation sequence. By default, <Print Screen> and Ctrl-Ctrl are set as the OSCAR activation options. Shift-Shift and Alt-Alt must be set within the OSCAR interface before use.
F1	Opens the Help screen for the current dialog box.
Escape	Closes the current dialog box without saving changes and returns to the previous one. If the Main dialog box is displayed, pressing Escape closes the OSCAR interface and displays a status flag if status flags are enabled. See the <i>Commands Dialog Box Functions</i> on page 25 for more information. In a message box, pressing Escape closes the pop-up box and returns to the current dialog box.
Alt	Opens dialog boxes, selects or checks options and executes actions when used with underlined or other designated letters.
Alt+X	Closes current dialog box and returns to previous one.
Alt+O	Selects the <i>OK</i> button, then returns to the previous dialog box.
Enter	Completes a switch operation in the Main dialog box and exits the OSCAR interface.
Single-click, Enter	In a text box, single-clicking an entry and pressing Enter selects the text for editing and enables the Left and Right Arrow keys to move the cursor. Press Enter again to quit the Edit mode.
Print Screen, Backspace	Toggles back to previous selection.
Print Screen, Alt+0 (zero)	Immediately disengages user from a target device; no target device is selected. Status flag displays <i>Free</i> . (This only applies to the 0 (zero) on the keyboard and not the numeric keypad.)
Print Screen, Pause	Immediately turns on Screen Saver mode and prevents access to that specific console, if it is password protected.
Up/Down Arrows	Moves the cursor from line to line in lists.
Right/Left Arrows	Moves the cursor between columns. When editing a text box, these keys move the cursor within the column.
Page Up/Page Down	Pages up and down through Name and Port lists and Help pages.
Home/End	Moves the cursor to the top or bottom of a list.
Backspace	Erases characters in a text box.

Table 3.3: OSCAR Interface Navigation Basics (Continued)

Keystroke	Function
Delete	Deletes current selection in the Scan list or characters in a text box.
Shift-Del	Deletes from the current selection to the end of the list when editing a Scan list.
Numbers	Type from the keyboard or keypad.
Caps Lock	Disabled. Use the Shift key to change case.
Backspace	Erases characters in a text box.

Setup Dialog Box Functions

You can configure your AutoView 3008/3016 switching system from the Setup dialog box within the OSCAR interface. Select the *Names* button when initially setting up your AutoView 3008/3016 switching system to identify target devices by unique names. Select the other setup features to manage routine tasks for your target devices from the OSCAR interface menu. Table 3.4 outlines the function accessed using each of the buttons in the Setup dialog box as shown in Figure 3.2.

Table 3.4: Setup Features to Configure the OSCAR Interface

Feature	Purpose
Menu	Change the Main dialog box list sorting option by toggling between numerically by port or EID number and alphabetically by name. Change the Screen Delay Time before the OSCAR interface displays after pressing Print Screen . You can also change how the OSCAR interface activation sequence is invoked.
Security	Set passwords to protect or restrict access or enable the screen saver.
Flag	Change display, timing, color or location of the status flag.
Devices	Identify the appropriate number of ports on an attached cascade switch.
Names	Identify target devices by unique names.
Keyboard	Set the keyboard country code to send to Sun servers.
Network	Choose your network speed, transmission mode and configuration.
Scan	Set up a custom Scan pattern for multiple target devices.

To access the OSCAR interface Setup dialog box, click *Setup* on the Main dialog box.



Figure 3.2: OSCAR Interface Setup Dialog Box

Changing the display behavior

Use the Menu dialog box to change the display order of target devices, change how the OSCAR interface is invoked or set a Screen Delay Time for the OSCAR interface. This setting alters how target devices will display in several dialog boxes, including Main, Devices and Scan List.

To access the OSCAR interface Menu dialog box, activate the OSCAR interface and click *Setup - Menu* in the Main dialog box.

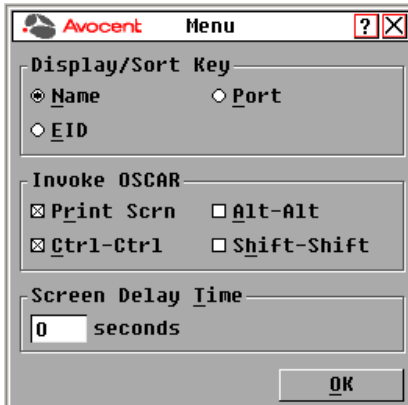


Figure 3.3: OSCAR Interface Menu Dialog Box

To choose the display order of target devices:

1. Select *Name* to display target devices alphabetically by name.
-or-
Select *EID* to display target devices numerically by EID number.

-or-

Select *Port* to display target devices numerically by port number.

2. Click *OK*.

Depending on the display method selected, the corresponding button will be depressed in the Main dialog box.

To change how the OSCAR interface is invoked:

1. Select the checkbox next to one of the listed methods.
2. Click *OK*.

To set a Screen Delay Time for the OSCAR interface:


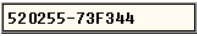

1. Type in the number of seconds (0-9) to delay the OSCAR interface display after you press **Print Screen**. Entering **0** will instantly launch the OSCAR interface with no delay.
2. Click *OK*.

Setting a Screen Delay Time enables you to complete a soft switch without the OSCAR interface displaying. To perform a soft switch, see the *Soft switching* on page 15.

Controlling the status flag

The status flag displays on your desktop and shows the name or EID number of the selected target device or the status of the selected port. Use the Flag dialog box to configure the flag to display by target device name or EID number, or to change the flag color, opacity, display time and location on the desktop. Table 3.5 describes each status flag.

Table 3.5: OSCAR Interface Status Flags

Flag	Description
	Flag type by name
	Flag type by EID number
	Flag indicating that the user has been disconnected from all systems

To access the OSCAR interface Flag dialog box:

1. Activate the OSCAR interface and click *Setup - Flag* to open the Flag dialog box.



Figure 3.4: OSCAR Interface Flag Dialog Box

To determine how the status flag is displayed:

1. Select *Name* or *EID* to determine what information will be displayed.
2. Select *Displayed* to activate the flag display. After a switch, the flag will remain on the screen until the user switches to another device. Selecting *Timed* will cause the flag to display for five seconds when a switch is made and then disappear.
3. Select a flag color under Display Color. The following flag colors are available:
 - *Flag 1* - Gray flag with black text
 - *Flag 2* - White flag with red text
 - *Flag 3* - White flag with blue text
 - *Flag 4* - White flag with violet text
4. In Display Mode, select *Opaque* for a solid color flag or *Transparent* to see the desktop through the flag.
5. To position the status flag on the desktop:
 - a. Click *Set Position* to gain access to the Position Flag screen shown in Figure 3.5.



Figure 3.5: Position Flag

- b. Left-click on the title bar and drag to the desired location.
- c. Right-click to return to the Flag dialog box.

NOTE: Changes made to the flag position are not saved until you click *OK* in the Flag dialog box.

6. Click *OK* to save settings.
-or-
Click *X* to exit without saving changes.

Setting the keyboard country code

NOTE: Using a keyboard code that supports a language different from that of your AutoView 3008/3016 switch firmware will cause incorrect keyboard mapping.

Sun servers may use keyboard mappings for non-US keyboards. By default, the AutoView 3008/3016 switch sends the US keyboard country code to Sun and USB modules attached to target devices, and the code is applied to the target devices when they are turned on or rebooted. Codes are then stored in the IQ module.

Issues may arise when you use the US keyboard country code with a keyboard of another country. For example, the **Z** key on a US keyboard is in the same location as the **Y** key on a German keyboard. Sun servers will interpret pressing the **Y** key on a German keyboard as pressing the **Z** key when the US keyboard country code is used.

The Keyboard dialog box enables you to send a different keyboard country code than the default US setting. The specified country code is sent to all target devices attached to the AutoView 3008/3016 switches when they are turned on or rebooted, and the new code is stored in the IQ module.

NOTE: If an IQ module is moved to a different target device, the keyboard country code will need to be reset.

See *Sun Advanced Key Emulation* on page 95 for information on emulating certain Sun keys using a PS/2 keyboard and special considerations for Japanese and Korean Sun USB keyboards.

NOTE: Only local users can view or change keyboard country code settings.

To set the keyboard country code for Sun servers:

1. Activate the OSCAR interface and click *Setup - Keyboard* to open the Keyboard dialog box shown in Figure 3.6.



Figure 3.6: OSCAR Interface Keyboard Dialog Box

2. Select a country code and click *OK* to save your settings.

3. Reboot the Sun servers. After rebooting, each Sun server will request the country code setting stored in the IQ module.

NOTE: If you wish to reboot the target devices by power-cycling them, you must wait 90 seconds before rebooting. A soft reboot may be performed without waiting 90 seconds.

Configuring network settings

Use the Network dialog box to set the Network Speed, Transmission Mode and Network Configuration feature.

To change network settings:

1. If the OSCAR interface is not open, press **Print Screen** to open the Main dialog box.
2. Click *Setup - Network* to open the Network dialog box.

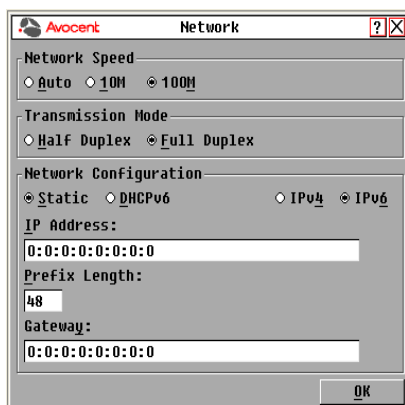


Figure 3.7: OSCAR Interface Network Dialog Box

3. Make desired changes and click *OK* to confirm or click *X* to exit without saving.

NOTE: Changing the network settings will cause the switch to reboot.

Assigning device types

To access the OSCAR interface Devices dialog box:

1. Activate the OSCAR interface and click *Setup - Devices* to open the Devices dialog box shown in Figure 3.8.

NOTE: The Modify button is available only if a configurable switch is selected.

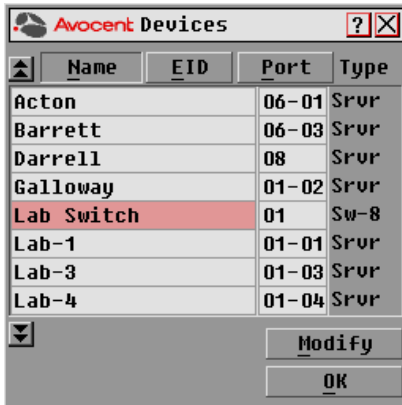


Figure 3.8: OSCAR Interface Devices Dialog Box

When the AutoView 3008/3016 switch discovers a cascaded switch, the numbering format changes from an AutoView 3008/3016 port only to [AutoView 3008/3016 port]-[switch port] to accommodate each target device under that switch.

For example, if a switch is connected to AutoView 3008/3016 port 6, each target device connected to it would be numbered sequentially. The target device using AutoView 3008/3016 port 6, switch port 1, would be 06-01, the target device using AutoView 3008/3016 port 6, switch port 2, would be 06-02, and so on.

To assign a device type:

1. In the Devices dialog box, select the desired port number.
2. Click *Modify* to open the Device Modify dialog box shown in Figure 3.9.

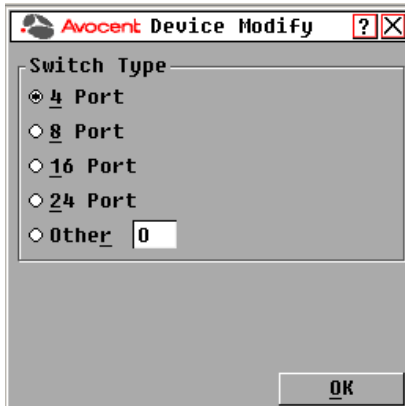


Figure 3.9: OSCAR Interface Device Modify Dialog Box

3. Choose the number of ports supported by your switch and click *OK*.

4. Repeat steps 1-3 for each port requiring a device type to be assigned.
5. Click *OK* in the Devices dialog box to save settings.

NOTE: Changes made in the Device Modify dialog box are not saved to the switch until you click *OK* in the Devices dialog box.

Assigning target device names

Use the Names dialog box to identify target devices by name rather than by port number. The Names list is always sorted by port order. You can toggle between displaying the name or the EID number of each IQ module, so even if you move the target device to another port, the name and configuration will be recognized by the switch.

NOTE: When it is initially connected, a target device will not appear in the Names list until it is turned on. Once an initial connection has been made, it will appear in the Names list even when turned off.

To access the OSCAR interface Names dialog box, activate the OSCAR interface and click *Setup - Names*.

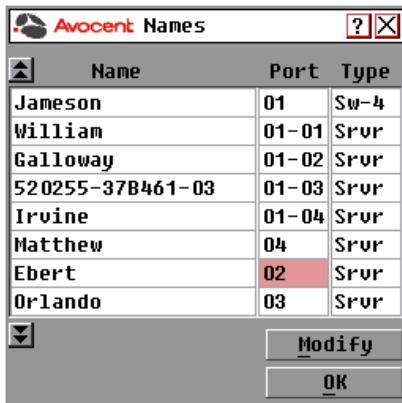


Figure 3.10: OSCAR Interface Names Dialog Box

NOTE: If new IQ modules are discovered by the AutoView 3008/3016 switch, the on-screen list will be automatically updated. The mouse cursor will change into an hourglass during the update. No mouse or keyboard input will be accepted until the list update is complete.

To assign names to target devices:

1. In the Names dialog box, select a target device name or port number and click *Modify* to open the Name Modify dialog box shown in Figure 3.11.



Figure 3.11: OSCAR Interface Name Modify Dialog Box

2. Type a name in the New Name box. Names of target devices may contain all printable characters.
 3. Click *OK* to assign the new name.
 4. Repeat steps 1-3 for each target device in the system.
 5. Click *OK* in the Names dialog box to save your changes.
- or-
- Click *X* or press **Escape** to exit the dialog box without saving changes.

NOTE: Changes made in the Names Modify dialog box are not saved to the switch until you click *OK* in the Names dialog box.

NOTE: If an IQ module has not been assigned a name, the EID is used as the default name.

Commands Dialog Box Functions

From the OSCAR interface Commands dialog box, you can manage your AutoView 3008/3016 switching system and user connections, enable the Scan mode and update your firmware.

Table 3.6: Commands to Manage Routine Tasks for Your Target Devices

Features	Purpose
Scan Enable	Begin scanning your target devices. Set up a target device list for scanning in the Setup dialog box. You must have at least two target devices selected in the Setup - Scan List menu to enable target scanning.
User Status	View and disconnect users.
AVRIQ Status	Displays the currently available firmware for each type of AVRIQ module.

Table 3.6: Commands to Manage Routine Tasks for Your Target Devices (Continued)

Features	Purpose
Display Versions	View version information for the AutoView 3008/3016 switch as well as view and upgrade firmware for individual IQ modules.
Display Config	View current configuration parameters.
Device Reset	Re-establish operation of PS/2 keyboard and mouse on the local port.

To access the OSCAR interface Commands dialog box:

Activate the OSCAR interface and click *Commands* to open the dialog box shown in Figure 3.12.

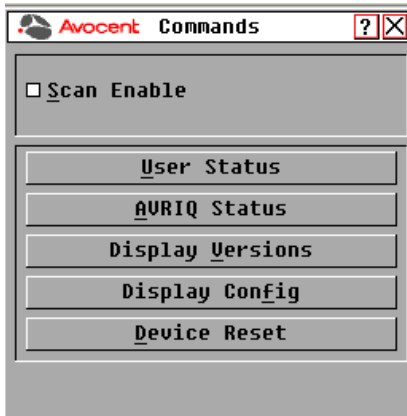


Figure 3.12: OSCAR Interface Commands Dialog Box

Selecting target devices for Scan mode

The Scan dialog box allows the local user to define a custom list of servers to include while in Scan mode and the number of seconds to display each server. The creation of the Scan list does not start Scan mode. You must enable Scan mode via the Scan Enable checkbox on the Commands dialog box. The Scan list is displayed in the manner set from the Menu dialog box. It can be changed in the Scan dialog box to sort either by Name, EID or Port by choosing one of the buttons. If a server on the list is unavailable, it is skipped. Watch mode views a server unless a conflicting network user blocks the path to that server. If a conflict is detected in Watch mode (or the server is unavailable), the server to be viewed is skipped.

To add target devices to the Scan list:

1. Activate the OSCAR interface and click *Setup - Scan* to open the Scan dialog box.

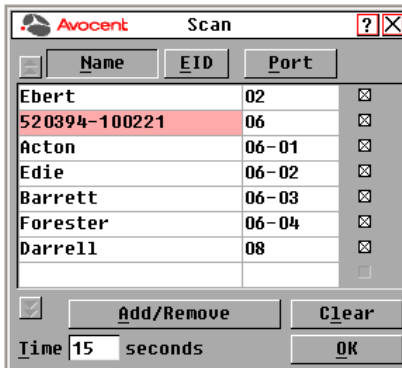


Figure 3.13: Scan Dialog Box

- The dialog box contains a listing of all servers attached to your switch. Click the checkbox to the right of the server, double-click on the desired entry, or highlight the device and click the *Add/Remove* button to toggle the scan checkbox setting. You can select up to 100 servers for inclusion in the Scan list.

NOTE: Click the *Clear* button to remove all servers from the Scan list.

- In the Time field, type the number of seconds (from 3 - 255) to display each server while scanning. The default is 15 seconds per server.
- Click *OK*.

NOTE: The order in which the servers appear in the Scan dialog box is based on the order in which they were selected. Scanning a single server multiple times during a loop is not supported. Scan time must be the same for all servers.

Enabling or disabling Scan mode

To start the Scan mode:

- Activate the OSCAR interface and click *Commands*. The Commands dialog box displays.
- Select *Scan Enable* in the Commands dialog box. Scanning will begin.
- Click *X* to close the Commands dialog box.

To cancel Scan mode:

Select a target device if the OSCAR interface is open.

-or-

Move the mouse or press any key on the keyboard if the OSCAR interface is not open. Scanning will stop at the currently selected target device.

-or-

From the Commands dialog box, deselect the *Scan Enable* checkbox.

Viewing and disconnecting user connections

You can view and disconnect users through the User Status dialog box. The username (U) and server (S) will always be displayed when connected to a target device (local or remote). You can display either the target device name or EID number to which a user is connected. If there is no user currently connected to a channel, the username and server fields will be blank.

To view current user connections, activate the OSCAR interface and click *Commands - User Status* to open the User Status dialog box shown in Figure 3.14.

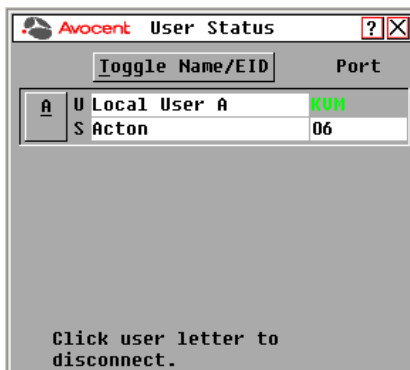


Figure 3.14: OSCAR Interface User Status Dialog Box

To disconnect a user:

1. On the User Status dialog box, click the letter corresponding to the user to disconnect. The Disconnect dialog box will appear as shown in Figure 3.15.

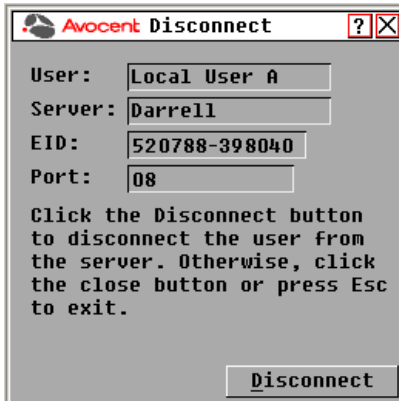


Figure 3.15: OSCAR Interface Disconnect Dialog Box

2. Click *Disconnect* to disconnect the user and return to the User Status dialog box.
-or-
Click *X* or press **Escape** to exit the dialog box without disconnecting a user.

Displaying version information and upgrading firmware

For troubleshooting and support, the OSCAR interface enables you to display the version number of the switch firmware and any auxiliary devices connected to the switch, as well as upgrade your firmware.

NOTE: For optimum performance, keep your firmware current.

To display version information and upgrade firmware:

1. Activate the OSCAR interface and click *Commands - Display Versions*. The top half of the box lists the subsystem version in the switch. The lower half displays the current IP address, Mask, MAC and EID.
2. If you want to upgrade the firmware, click *Upgrade* and then click *OK* to open the download box. You will be prompted for an FTP or TFTP server IP address and the related information.
3. Click *Download*. After the firmware is downloaded, the Upgrade dialog box will appear.
4. Click the *Upgrade* button.

NOTE: The switch will reboot when the upgrade is complete.

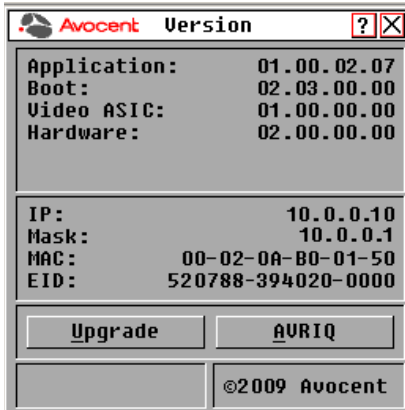


Figure 3.16: OSCAR Interface Version Dialog Box

- To upgrade individual IQ modules, click the *AVRIQ* button to view individual AVRIQ module version information.

NOTE: To upgrade multiple AVRIQ modules simultaneously, go to step 9.

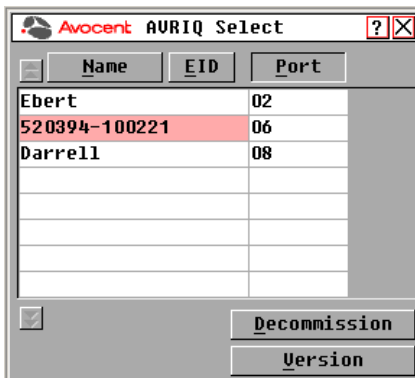


Figure 3.17: AVRIQ Selection Dialog Box

6. Select an AVRIQ module to view and click the *Version* button..

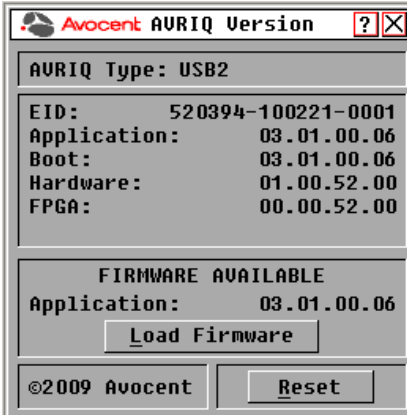


Figure 3.18: AVRIQ Version Dialog Box

7. Click the *Load Firmware* button.
8. Click *OK* to initiate the upgrade and return to the Status dialog box.

NOTE: During an upgrade, the AVRIQ module status indicator in the Main dialog box is yellow. The AVRIQ module is unavailable when an upgrade is in progress. When an upgrade is initiated, any current connection to the server via the AVRIQ module is terminated.

9. To simultaneously upgrade multiple AVRIQ modules, activate the OSCAR interface, click *Commands - AVRIQ Status* and click one or more types of modules to upgrade. Click *Upgrade*.

NOTE: When the Enable AVRIQ Autoupdate option is enabled in the AVRIQ Status dialog box, AVRIQ module firmware is automatically upgraded when the AutoView 3008/3016 switch firmware is upgraded or when a new AVRIQ module is discovered by the AutoView 3008/3016 switch after a firmware upgrade. AVRIQ modules that have already been discovered but which are not attached to the AutoView 3008/3016 switch during the firmware upgrade must be upgraded manually.

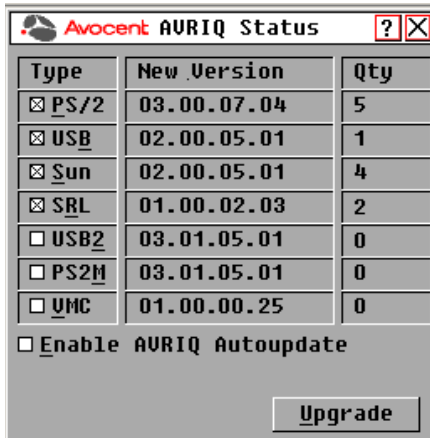


Figure 3.19: AVRIQ Status Dialog Box

10. The AVRIQ Upgrade dialog box displays. Click *OK* to initiate the upgrade and return to the AVRIQ Status dialog box.

Returning an AVRIQ module to factory default status:

1. Click *AVRIQ* in the Version dialog box.
2. Select an AVRIQ and click *Decommission*.
3. Click *OK* to restore factory defaults. You will see the AVRIQ module go offline briefly and return.
- or -
Click *X* or press *Escape* to cancel the operation.
4. Click *X* to close the AVRIQ Select dialog box.

Resetting the PS/2 keyboard and mouse on a target device or local port

NOTE: This function is for Microsoft Windows-based computers only. Resetting the PS/2 ports on a target device running any other operating system may require that you reboot that target device.

If your PS/2 keyboard or mouse locks up, you may be able to re-establish operation of these peripherals by issuing a Reset command. The Reset command sends a hot-plug sequence to the target device that requests the mouse and keyboard settings from the target device to restore functionality.

To issue a remote PS/2 reset command:

1. Select an individual IQ module in the AVRIQ Select dialog box and click *Version*. From the AVRIQ Version dialog box, click *Reset*. A confirmation message will appear.

2. On the message box, click *X* or press **Escape** to exit without sending a Reset command to the target device.

To reset the local mouse and keyboard:

1. Activate the OSCAR interface and click *Commands - Device Reset*. A confirmation message will appear.
2. Click *X* or press **Escape** to clear the message.

Web Interface Operations

AutoView 3008/3016 Switch OBWI

In addition to the OSCAR interface, AutoView 3008/3016 switches are equipped with an On-Board Web Interface (OBWI) feature that provides a built-in interface to handle all basic KVM switching needs. The AutoView 3008/3016 switch OBWI provides secure “point-and-click” web browser-based access to control any device attached to your AutoView 3008/3016 switch.

Table 4.1 shows which operating systems and browsers the AutoView 3008/3016 switch OBWI supports.

Table 4.1: OBWI Supported Operating Systems and Browsers

Operating System	Browser		
	Microsoft Internet Explorer version 6.0 SP1 and later	Mozilla® version 1.7.3 and later	Firefox® version 1.0 and later
Windows Server® 2003 SP1 Standard, Enterprise or Web Edition	Yes	Yes	Yes
Windows Vista Business	Yes	Yes	Yes
Windows Server 2008	Yes	Yes	Yes
Windows XP Home Edition or Professional SP2	Yes	Yes	Yes
Red Hat® Enterprise Linux 3, 4 and 5	No	Yes	Yes
Sun® Solaris™ 9 and 10	No	Yes	Yes
Novell® SUSE® Linux Enterprise Server 10	No	Yes	Yes

NOTE: Avocent recommends your browser be kept up-to-date with the latest version.

A Video Viewer window provides real-time control of the keyboard, monitor and mouse functions of individual target devices connected to the AutoView 3008/3016 switch. You may also use

predefined global macros to perform actions within the Video Viewer window. For instructions on how to use the Video Viewer, see Chapter 5.

Viewing and Selecting Ports and Servers

Before you can begin a KVM session, you must first log in to the AutoView switch OBWI.

To log in to the AutoView 3008/3016 switch OBWI:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the AutoView 3008/3016 switch you wish to access. Use `https://xxx.xx.xx.xx` or `https://hostname` as the format.
3. When the browser makes contact with the switch, enter your username and password, then click *Login*. The AutoView 3008/3016 Explorer window will appear.

NOTE: The default username is **Admin** with no password.

The AutoView 3008/3016 Explorer Window

When a user has been logged in and authenticated, the Avocent AutoView 3008/3016 Explorer window appears. From the AutoView 3008/3016 Explorer window, users may view, access and manage their AutoView 3008/3016 switch, specify system settings and change profile settings.

Figure 4.1 shows the AutoView 3008/3016 Explorer window areas and descriptions follow in Table 4.2.

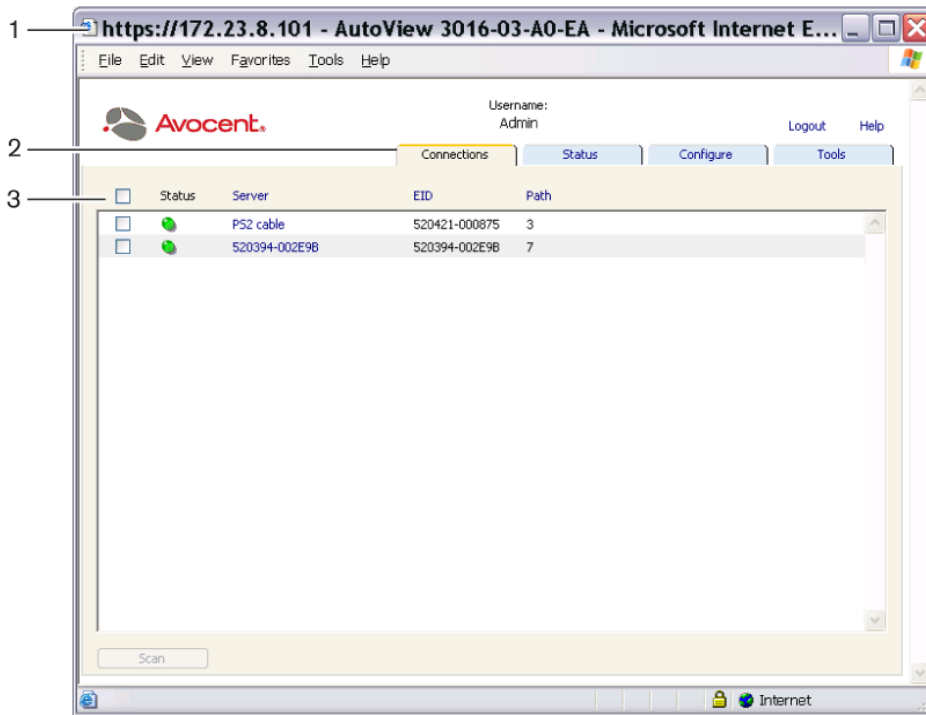


Figure 4.1: Avocent AutoView 3016 Explorer Window

Table 4.2: Descriptions for Figure 4.1

Number	Description
1	Displays the IP address, appliance type and last six digits of the appliance MAC address and browser being accessed.
2	OBWI tabs used to display connections, status and configure the appliance.
3	Shows connected IQ modules, including Status, Server (which is a hyper link allowing access to the target server selected), EID and Path to targets connected to the switch.

Launching a KVM Session

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as Grayscale) use less network bandwidth than others (such as Best Color), changing the color settings can increase video performance. For optimal video performance over a slower network connection, Avocent recommends a color setting such as Grayscale/Best Compression or Low Color/High Compression.

NOTE: If a user connects to a target device with a higher screen resolution than the local computer, the Video Viewer window will display a portion of the target device screen, with scroll bars for viewing the remainder of the screen. The user may view the entire screen by adjusting the resolution on the target device, the local computer or both.

To launch a KVM session from the AutoView 3008/3016 Explorer browser window:

Click on a device listed on the Connections tab to open the Video Viewer in a new window.

For more information on launching a session when sharing is enabled, see *Session sharing options* on page 39.

For more information on using the Video Viewer, see Chapter 5.

Viewing and terminating user sessions

You may view and disconnect the current active user connections using the Status tab in the OBWI. You can view the session type, the server name, or IQ module to which they are connected and their system address. In addition to disconnecting a user session, the AutoView switch also allows one user to take control of a server currently being used by another user.

To disconnect a user session:

1. Click the *Status* tab in the OBWI. A list of users and their connection information appears.

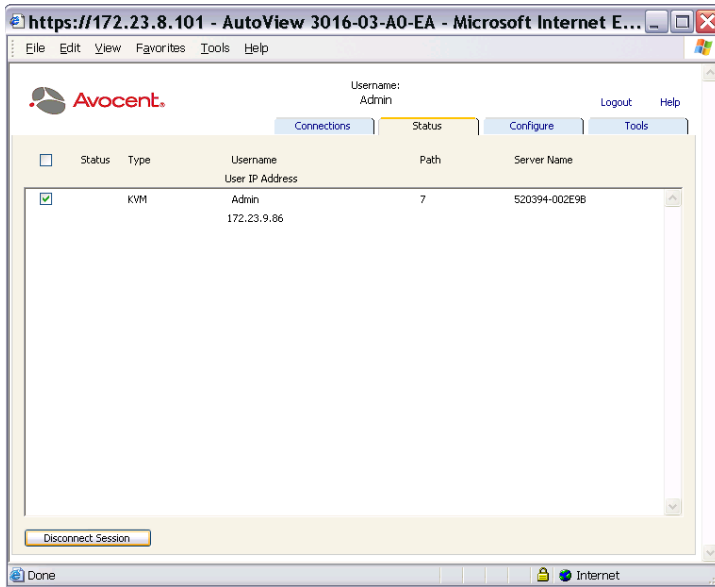


Figure 4.2: Disconnect Session Status Window

2. Click the checkbox for one or more users that you wish to disconnect.
3. Click the *Disconnect Session* button. A message appears prompting you to confirm the disconnect command.
4. Click *OK* to disconnect the user.
-or-
Click *Cancel* to exit without completing the disconnect command.

NOTE: The appropriate level of access is required to disconnect a user. If you do not have permission to disconnect a user, the checkbox next to that user will be disabled.

Session sharing options

Session sharing can be configured by Admin and other users with Appliance Administrator or User Administrator rights. The first user with a KVM session with a target device is called the primary user. If another (secondary) user attempts to start a KVM session the same target device, options for the secondary user depend on the following two conditions:

- The access rights of the users

- Whether an Administrator has configured global connection sharing (Automatic Sharing, Exclusive Connections and Stealth Connections all are configurable options that require sharing to be enabled)

Table 4.3: Session Sharing Definitions

Term	Definition
Automatic Sharing	Secondary users can share a KVM session without first requesting permission from primary users.
Exclusive Connections	Primary users can designate a KVM session as an exclusive connection that cannot be shared.
Stealth Connections	Stealth connections allow undetected viewing of KVM sessions. Secondary users with Appliance Administrator rights can create stealth connections to any KVM session. Secondary users with User Administrator rights can create stealth connections when their access rights are the same as or higher than the rights of the primary user. Stealth permissions follow preemption permissions.
Preempt Mode	Secondary users with Appliance Administrator rights can preempt sessions. Secondary users with User Administrator rights can preempt sessions only when their access rights are the same as or higher than the rights of the primary user.

To connect to target devices when sharing is enabled:

1. Log into the OBWI as any user configured for access to one or more target devices. The Explorer window appears with the Connections tab active.
2. Click the name of a target device. A Video Session Viewer information dialog box briefly appears followed by a status dialog box.
3. If another user does not have an active KVM session with the target device, the Video Viewer window appears.

-or-

If another user has an active KVM session with the target device, and sharing is not enabled, or if the number of port sessions has been exceeded, a message window displays and you are denied access to the target device.

4. If sharing is enabled, you can have several options depending on your access rights and on whether session sharing, session preemption, or Stealth Connections are enabled.
 - If you have Appliance Administrator rights, you can share any session, preempt the session, or observe the session with stealth connections.
 - If you have User Administrator rights, you can share the session, preempt the session, or observe the session with Stealth Connections only if your rights are the same as or higher than the primary user.

- If an Administrator has enabled Exclusive Connections, and a primary user has set Exclusive Mode for the session, you cannot share the session unless you have Appliance Administrator rights.
5. If an Administrator has enabled Exclusive Connections, you can click the *Exclusive Mode* option in the Video Viewer toolbar Tools menu. The Exclusive Mode status symbol appears in the toolbar.
 6. To end a KVM session, click *File-Exit* from the toolbar. See Chapter 5 for more information using the Video Viewer.

Managing the AutoView 3008/3016 switch OBWI

The AutoView 3008/3016 switch OBWI provides several configuration options to tailor the switch to your specific application.

Managing users

The AutoView 3008/3016 switch OBWI provides local and login security through administrator-defined user accounts. By selecting the *Configure* tab and then selecting *Users* on the side menu bar, administrators may add and delete users, define user preemption and access levels and change passwords.

Access levels

When a user account is added to the OBWI, the user may be assigned to any of the following access levels:

- Appliance Administrator
- User Administrator
- User

Table 4.4: Allowed Operations by Access Level

Operation	Access Level		
	Appliance Administrator	User Administrator	User
Configure OBWI system-level settings	Yes	No	No
Configure access rights	Yes	Yes	No
Add, change and delete user accounts	Yes, for all access levels	Yes, for users and user administrators only	No
Change your own password	Yes	Yes	Yes
Access target device	Yes, all target devices	Yes, all target devices	Yes, if allowed

Setting up user accounts

When you select the *Users* category, the OBWI will retrieve and display a list of usernames and current access levels from the AutoView switch. From here, you can add, modify or delete users and assign access levels. The User Administrator and Appliance Administrator access levels allows you to assign individual server access rights.

Table 4.5: User Access Level Rights

Operations	Appliance Administrator	User Administrator	User
Preemption	All	Equal and lesser	No
Configure network & global settings [security mode, time-out, Simple Network Management Protocol (SNMP)]	Yes	No	No
Reboot	Yes	No	No
Flash upgrade	Yes	No	No
Administer User Accounts	Yes	Yes	No
Monitor server status	Yes	Yes	No
Target device access	Yes	Yes	Assigned by Admin

NOTE: Preemptions listed in the previous table only apply to remote clients. They do not apply to users accessing the server locally.

Users can become locked out by the Security Lock-out feature if they try to enter an invalid password five consecutive times. You can configure Security Lock-out settings as well as unlock any user through the User category.

Modifying users

To add or modify a user:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.

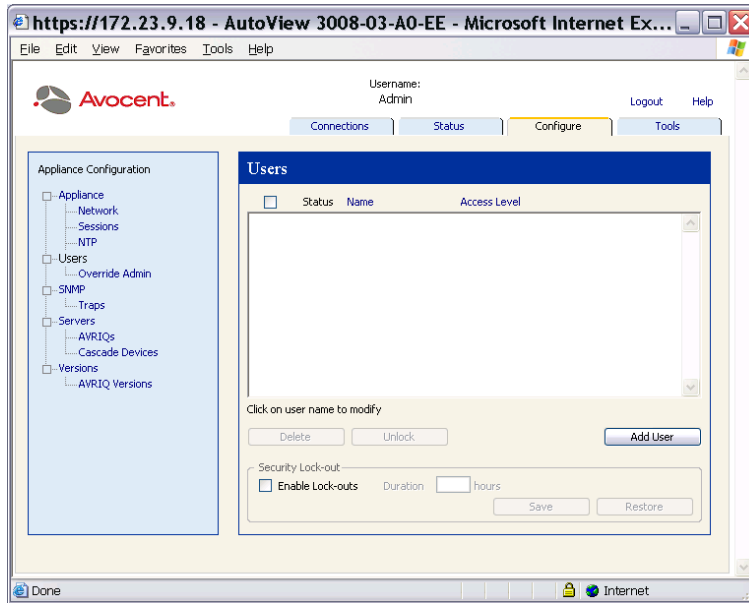


Figure 4.3: Users Window

2. Click the *Add User* button on the right side of the window to add a new user.
-or-
Click a username listed in the Users column to modify an existing user. The Add/Modify User window appears.

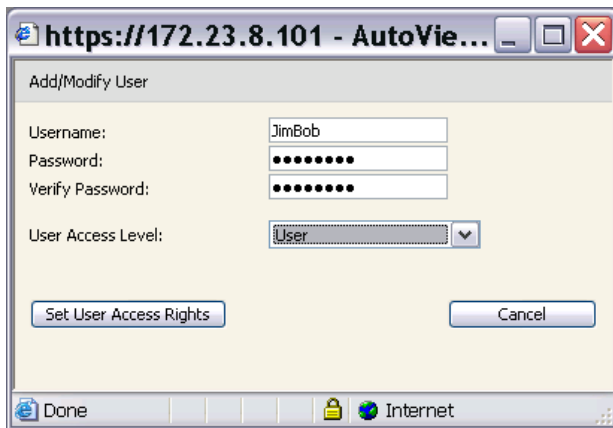


Figure 4.4: Add/Modify User Window

3. Type the username and password you wish to assign to the user and then verify the password by typing it in the Verify Password field. The password must be 5-16 characters and contain alphabetical characters of mixed case and at least one number.
4. Select the appropriate access level for this user from the drop-down list. If you select the *User* option, the Set User Access Rights button becomes active.
 - a. Click the *Set User Access Rights* button to select individual servers for that user. The User Access Rights window appears.
 - b. To allow the user access to a server, select the checkbox next to the server name. Alternatively, you may select the first checkbox to enable access on all servers.
 - c. To prevent the user from accessing a server, clear the checkbox next to the server name.
5. Click *Save* to save the settings and return to the main OBWI window.

To change a user password or access level:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Click the username you want to modify.
3. Enter the new password and/or access level in the provided fields.
4. Click *Save* to return to the OBWI.

To delete a user:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Select the checkbox next to the username you wish to delete.
3. Click the *Delete* button on the left side of the window. A confirmation window appears.
4. Click *Yes* to confirm the deletion.
-or-
Click *No* to exit the window without deleting the user.

To configure user rights to specific servers:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Click the username you want to modify.
3. Click the *Set User Access Rights* button.
4. Using the checkboxes in the left column, select the servers you want the user to be able to access.
5. Click *Save*.

Locking and unlocking user accounts

If a user enters an invalid password five consecutive times, the Security Lock-out feature, if enabled, will temporarily disable that account.

NOTE: All accounts (User, User Administrator and switch administrator) are subject to this lock-out policy.

A Switch Administrator can specify the number of hours (1 to 99) that accounts will remain locked. When Enable Lock-outs is unchecked, the Security Lock-out feature will be disabled and no users will be locked out.

If an account becomes locked, it will remain locked until the duration time has elapsed, the switch is power cycled or an administrator unlocks the account. A User Administrator may only unlock user accounts, while a Switch Administrator may unlock any type of account.

To enable or disable the Security Lock-out feature:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Select the *Enable Lock-outs* checkbox and enter a lock-out duration if necessary.

NOTE: Disabling Security Lock-out will have no affect on users that are already locked out.

To unlock an account:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Select the checkbox next to the username you wish to unlock.
3. Click the *Unlock* button. The lock icon next to the username will disappear.

To specify the length of time a user account remains locked:

1. Click the *Configure* tab in the OBWI, then click the *Users* category in the left column.
2. Click to enable the Enable Lock-outs checkbox.
3. Type the number of hours that a user will be locked out (1 to 99).

NOTE: Only switch administrators may specify lock-out parameters.

Managing Device Properties

Viewing and changing appliance configuration information

The AutoView 3008/3016 switch can report most device properties directly through the AutoView switch web browser.

The Configure tab allows you to display a list of categories covering a wide range of parameters for your switch. When a category is selected from the list, the parameters associated with the category will be read from the unit. You will then be able to modify those parameters and send the changes securely back to the switch.

Viewing switch parameters

The Appliance category allows you to view the Product Type, Product Name, Product Description, EID, MAC Address, Number of Digitizers, ARI Ports and Local Ports for the AutoView switch.

From the Network sub-category, you are able to modify the network configuration for the AutoView switch.

NOTE: After changing Network settings, the switch must be rebooted.

NOTE: Users can view all appliance information, but only Administrators can change settings.

The Sessions sub-category allows you to apply controls to your video sessions.

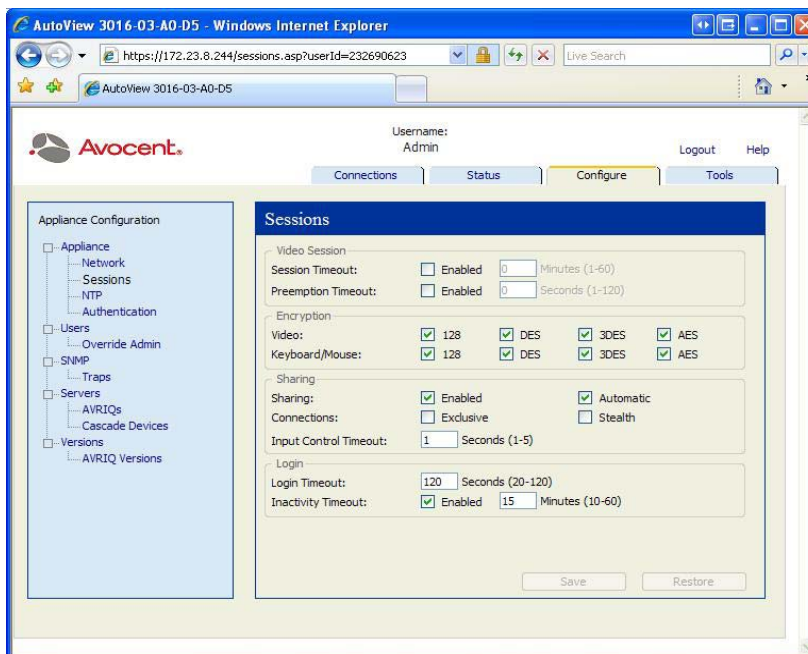


Figure 4.5: Sessions Window

Session time-out

By enabling the Video Session Timeout option, you allow the switch to close an inactive video session after a specified number of minutes. The Video Session Preemption Timeout option allows you to specify the time (5 - 120 seconds) for which a preemption warning message appears before a video session is preempted. If this option is not enabled, preemption occurs without warning.

To enable, disable or configure the session time-out:

1. Select the *Configure* tab, then select *Appliance - Sessions*.
2. Select the desired setting for the Session Timeout box.
3. If necessary, select the time limit for Inactivity Timeout.

NOTE: It is possible for two users to select the same server at the same time. Each may enter information at the same time, so care must be taken to avoid errors.

The Encryption option allows you to specify the type of encryption to be used for video, keyboard and mouse sessions. You can select multiple methods when a new client connection is requested. The AutoView 3008/3016 switch negotiates for the highest enabled encryption method.

The Login Timeout option specifies the time period allowed to respond to a log in request. The default time is 30 seconds, but some WANs may require a longer time period.

Enabling Network Time Protocol (NTP) functionality

NTP settings can be configured for your AutoView 3008/3016 switch. The switch must have access to the current time to verify that certificates have not expired and you can configure the switch to request time updates from the network time server (NTP).

To enable NTP functionality:

1. Click the *Configure* tab in the OBWI, then click *Appliance-NTP* in the left column.
2. Click the *Enable NTP* checkbox and enter the IP address for the NTP server you want to use, along with an update interval.
3. Click the *Save* button to exit, or *Restore* to leave the settings unchanged.

Configuring an Override Admin Account

As a failsafe measure, the AutoView switch can be configured with an administrator account that can be used to access the switch from a network, even if the local accounts are locked or the LDAP service has failed.

To configure an Override Admin Account:

1. Click the *Configure* tab in the OBWI, then click *Users-Override Admin* in the left column.
2. Enter a username and password for the Override Admin account and click *Save*.

Enabling and configuring SNMP

SNMP is a protocol used for communication between network management applications and your AutoView switch. Other SNMP managers can communicate with your AutoView switch by accessing MIB-II and the public portion of the enterprise MIB. When you select the SNMP category, the OBWI will retrieve the SNMP parameters from the unit.

In the SNMP category, you can enter system information and community strings. You may also designate which stations can manage your AutoView switch as well as receive SNMP traps from the switch.

NOTE: The OBWI does not use standard SNMP to control switches and therefore does not use UDP port 161. The OBWI uses a secure, proprietary protocol to communicate with the switch over a different network port. However, if you check the Enable SNMP checkbox, the unit will respond to SNMP requests over UDP port 161.

To configure general SNMP settings:

1. Click the *Configure* tab in the OBWI, then click the *SNMP* category in the left column.

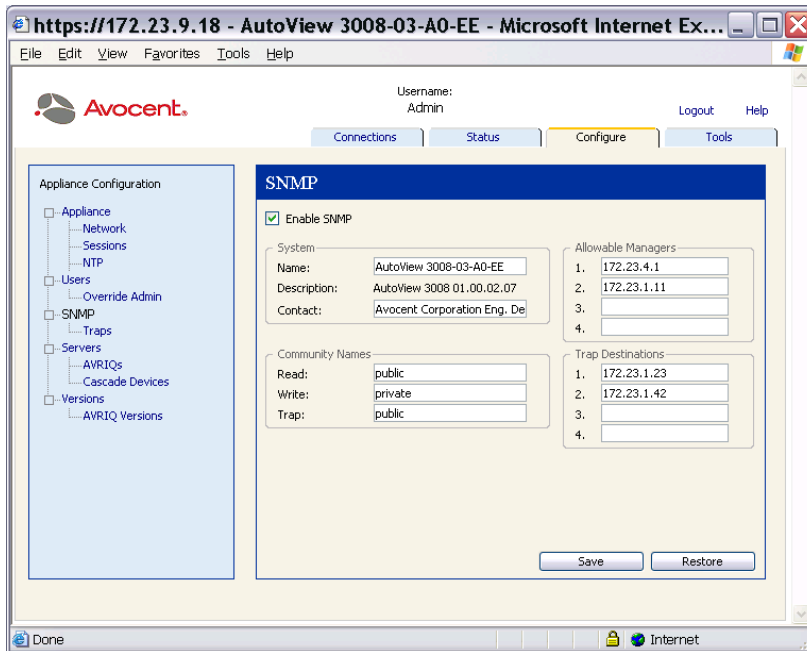


Figure 4.6: SNMP Window

2. Click the Enable SNMP checkbox to allow the AutoView switch to respond to SNMP requests over UDP port 161.
3. Type the system's fully qualified domain name in the Name field, as well as a node contact person in the Contact section.
4. Type the Read, Write and Trap community names. These specify the community strings that must be used in SNMP actions. The Read and Write strings only apply to SNMP over UDP port 161 and act as passwords that protect access to the AutoView switch. The values can be up to 64 characters in length. These fields may not be left blank.
5. Type the address of up to four management workstations that are allowed to manage this AutoView switch in the Allowable Managers fields. Leaving these fields blank allows any station to manage the switch.
6. In the Trap Destination fields, type the address of up to four management workstations to which this AutoView switch will send traps.
7. Click *Save* to save the settings and close the window.
-or-
Click *Restore* to cancel the changes and exit the window. The last saved settings will be restored.

NOTE: After changing SNMP settings, the switch must be rebooted. See *Rebooting the switch* on page 56 for more information.

Enabling individual SNMP traps

An SNMP trap is a notification sent by the AutoView switch to a management station indicating that an event has occurred that may require further attention. By selecting or clearing SNMP traps from the left column, you can specify what SNMP traps are sent to the management stations by clicking the appropriate checkboxes in the list. You can use the checkbox next to Enabled Traps to select or deselect the entire list.

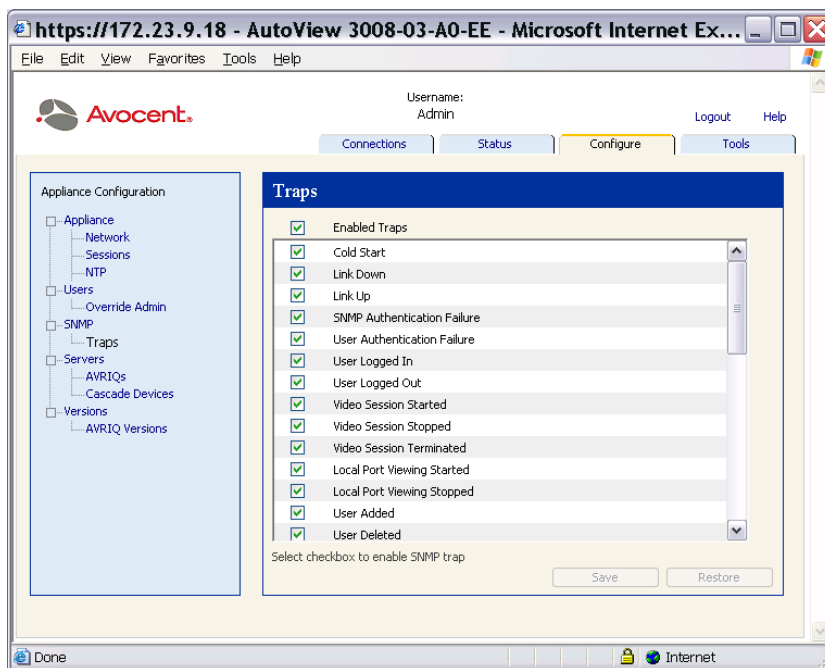


Figure 4.7: Traps Window

Viewing and resynchronizing server connections

The Servers category retrieves and displays the servers in the AutoView switch database as well as information on how the servers are connected to the selected switch.

The Path column displays the current server connection. This can be to either an IQ module or a cascaded switch. If connected to an IQ module, the IQ module's ARI port is displayed. If connected to a cascaded switch, the switch channel is also displayed.

Modifying a server name

You can use the OBWI to rename a server from a remote workstation rather than from the OSCAR interface.

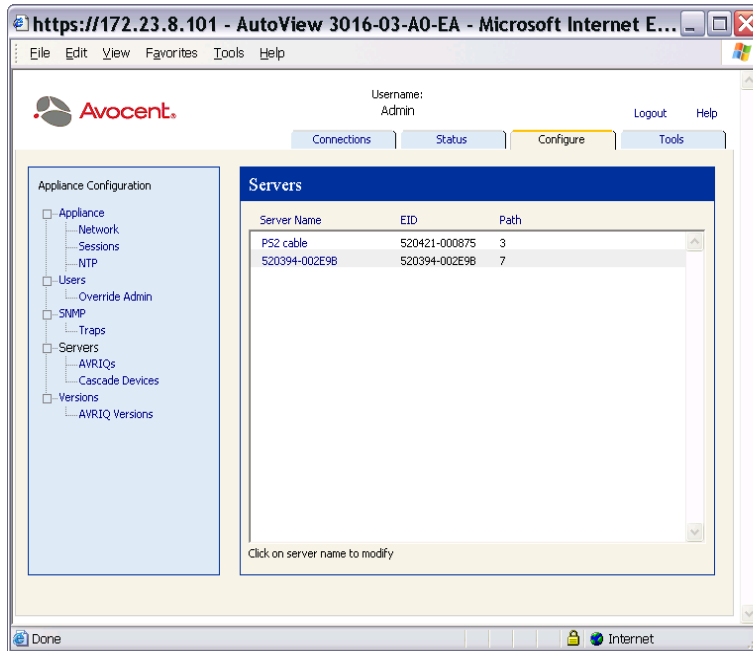


Figure 4.8: Servers Window

To modify a server name:

1. Click the *Configure* tab in the OBWI, then click *Servers-Cascade Devices* in the left column.

- In the Server Name column, click the server you want to modify.

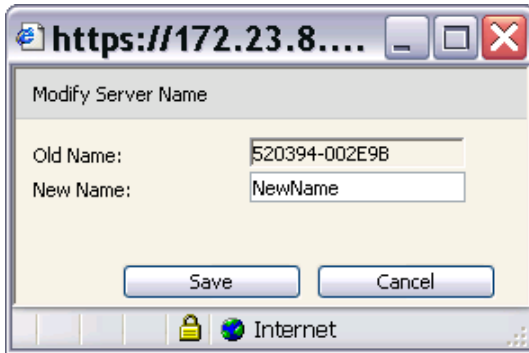


Figure 4.9: Modify Server Name Window

- Type the new name. Names must be 1-15 characters, include alphabetical characters, and may not include spaces or special characters with the exception of hyphens.
- Click *Save*. The new name is updated in both the AutoView switch and local client database.

Viewing the IQ modules and IACs

Selecting *Servers - AVRIQs* lets you view IQ modules and IACs in your system, their path, Electronic ID number (EID), their type and the device to which it is connected.

You can also view the IQ module status. A green circle indicates that the IQ module is online. A yellow circle indicates the IQ module is being upgraded and a red X indicates that the IQ module is offline. To clear offline IQ modules, click *Clear Offline AVRIQs* and click *OK* when prompted. The Clear Offline AVRIQs button is only available for AutoView switch administrators.

NOTE: It is not possible to clear offline IQ modules that are attached to a cascaded analog switch.

NOTE: User access rights will also be updated to remove the servers associated with the cleared offline IQ modules.

The AVRIQ Language drop-down menu allows you to set language and keyboard parameters for all the Sun/USB IQ modules being used with the switch. The AVRIQ Language drop-down menu is only available for switch administrators.

NOTE: The Reboot Required button will only appear if a reboot is required.

Viewing and configuring cascaded switch connections

The Cascaded Devices window lets you view the cascaded switches in your system. Clicking on a switch name displays a window that allows you to change the Name or Number of Channels.

To configure a cascaded switch connection:

1. Click the *Configure* tab in the OBWI, then click *Servers-Cascade Devices* in the left column.
2. Click the name of the switch you want to configure and type the new name for the cascaded device.
3. Type the number of channels, between 4-24, for the switch.
4. When you have finished configuring the switches, click *Save* to save the new settings.
-or-
Click *Cancel* to exit without saving.

Viewing version information

The Versions category displays versions of the AutoView switch, FPGA and ASIC firmware.

When you select the Version sub-category, the OBWI will retrieve the firmware versions from the selected AutoView 3008/3016 switch. This read-only information displays the version information for the unit itself. The AVR1Q Versions sub-category allows you to view and upgrade all of the IQ modules in the system.

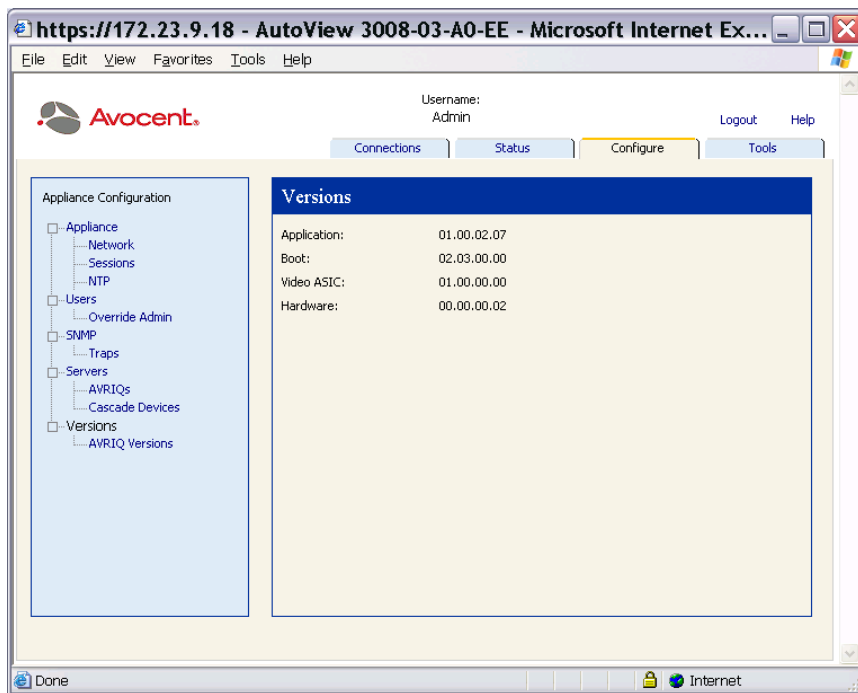


Figure 4.10: Versions Window

AVRIQ versions

The AVRIQ Versions sub-category allows you to view version information for attached AVRIQ modules. Clicking on the EID displays a window that allows you to upgrade the IQ module firmware and to reset the IQs if connected to a cascaded device.

Selecting the Enable Auto-Upgrade for all IQs checkbox causes all subsequently connected IQ modules to have their firmware upgraded to what is available on the AutoView switch. This guarantees that IQ module firmware is compatible with AutoView switch firmware.

When you select the *Versions* category, the OBWI will retrieve the firmware versions from the selected switch. The AVRIQ Versions sub-category allows you to view and upgrade all of the IQ modules and IACs in the system.

On occasions when a cascaded switch is not recognized by the AutoView switch, it may be necessary to reset the IQ module which connects the cascaded switch to the AutoView switch. This can be done using the Reset IQ module button in the IQs sub-category.

To view version information for AVRIQ modules:

1. Click the *Configure* tab in the OBWI, then click *Versions - AVRIQ Versions* in the left column.

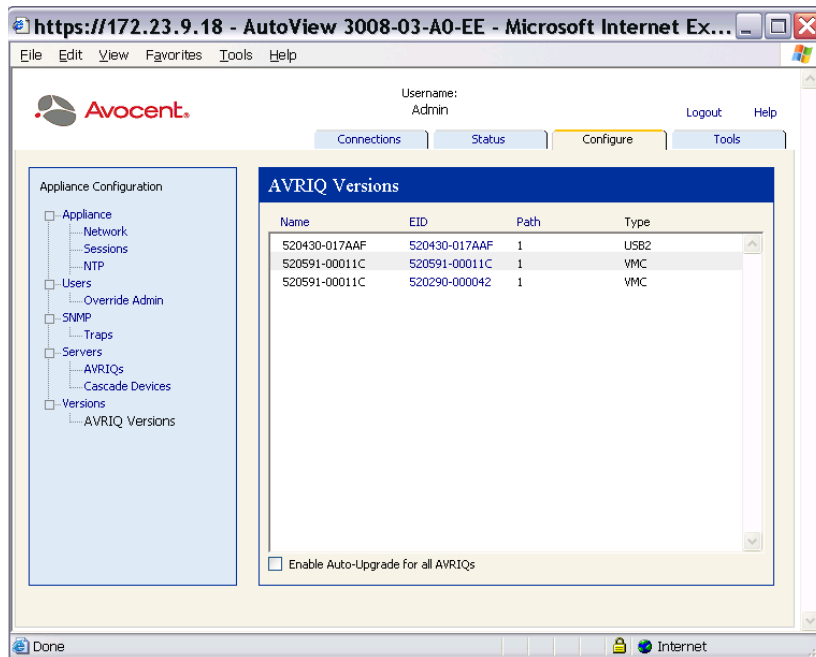


Figure 4.11: AVRIQ Versions Window

2. Click the EID of the AVRIQ module for which you want to view the firmware version.

NOTE: PS/2, USB and USB2 IQ modules are available. In addition, the AutoView switch is compatible with all Avocent IQ modules including Sun and serial IQ modules.

NOTE: Resetting an AutoView switch that is connected directly to a server (not a cascaded switch) may cause the mouse/keyboard to fail. When this occurs, reboot the target server.

To reset an AVRIQ module:

1. Click the *Configure* tab in the OBWI, then click *Versions - AVRIQ Versions* in the left column.
2. Click the EID of the AVRIQ module you want to reset.
3. Click *Reset*. A message appears warning you that this function is reserved for cascaded switches and that resetting the AVRIQ module may result in the need to reboot the server.
4. Click *OK* to continue.
-or-
Click *Cancel* to return to the AVRIQ Versions sub-category.

Upgrading firmware

You can upgrade the firmware for either the switch or the IQ modules. The IQ modules can be upgraded individually or simultaneously. When an appliance upgrade is initiated, you will see a progress bar. As long as an upgrade is in progress, you cannot initiate another.

The Enable Auto-Upgrade for all AVRIQs checkbox allows you to enable an auto-upgrade for IQ module firmware. You can override the auto-upgrade at any stage using the Load Firmware button described in the next section.

To upgrade appliance firmware:

1. Click the *Tools* tab in the OBWI.
2. Click the *Upgrade Appliance Firmware* button.
3. The Upgrade Appliance Firmware window appears. Select how the upgrade files will be supplied and the location of the upgrade files.
4. Click *Upgrade*.

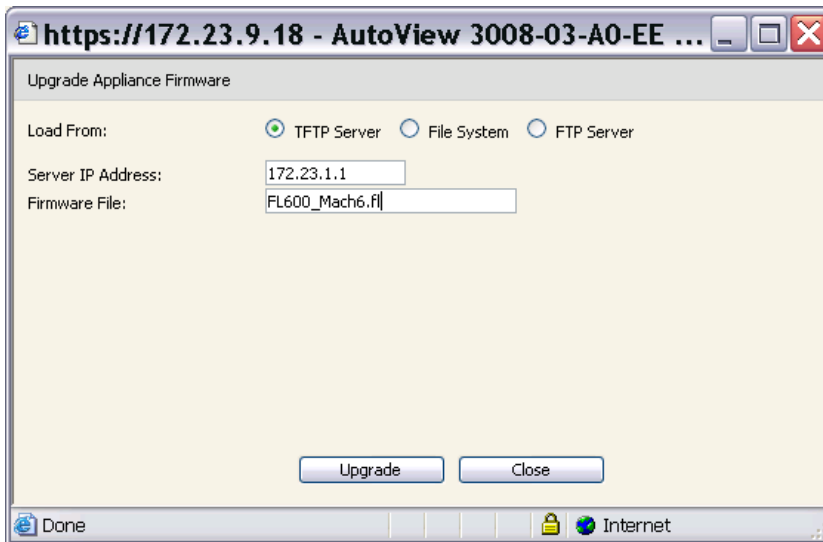


Figure 4.12: Upgrade Appliance Firmware (TFTP Server) Window

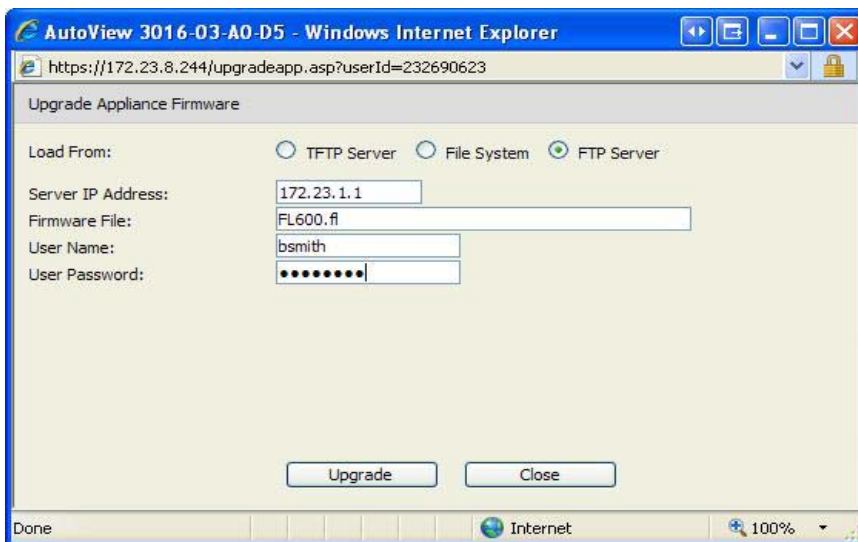


Figure 4.13: Upgrade Appliance Firmware (File System) Window

To upgrade AVRIQ module firmware:

1. Click the *Tools* tab.

2. Click the *Upgrade AVRIQ Firmware* button.
3. Select the module types you want to upgrade.
4. Click *Upgrade*.

Rebooting the switch

Periodically, such as after an upgrade, you may need to reboot the AutoView 3008/3016 switch. You can reboot the switch through the Tools tab in the OBWI. When clicked, *Reboot Appliance* will broadcast a disconnect message to any active users, then log out the current user and immediately reboot the AutoView switch.

To reboot the switch:

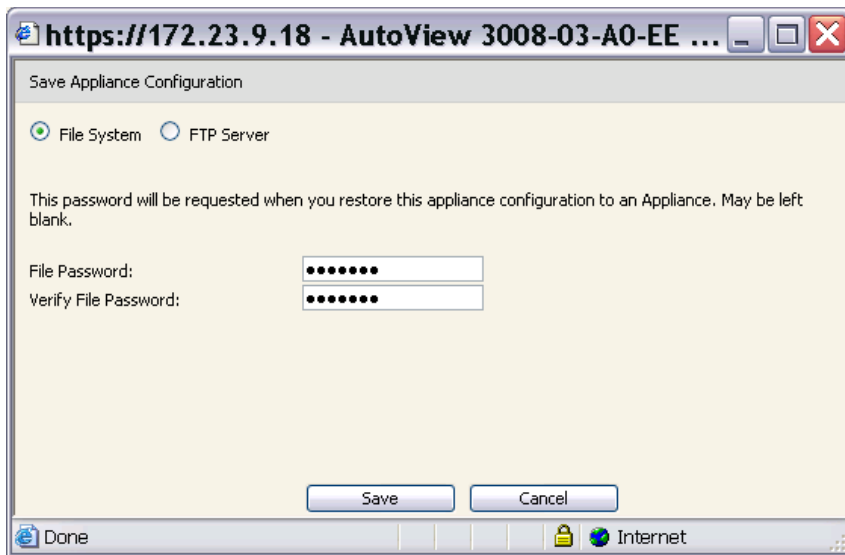
1. In the OBWI, click *Tools - Reboot Appliance*.
2. Click *OK* to reboot the appliance or *Cancel* to abort.

Managing AutoView switch configuration files

Configuration files contain all of the settings for a AutoView switch. This includes appliance settings, SNMP settings and NTP settings. You may save your configuration file and, should you ever need to replace your AutoView switch, you can restore the configuration file to the new switch and avoid manually configuring it.

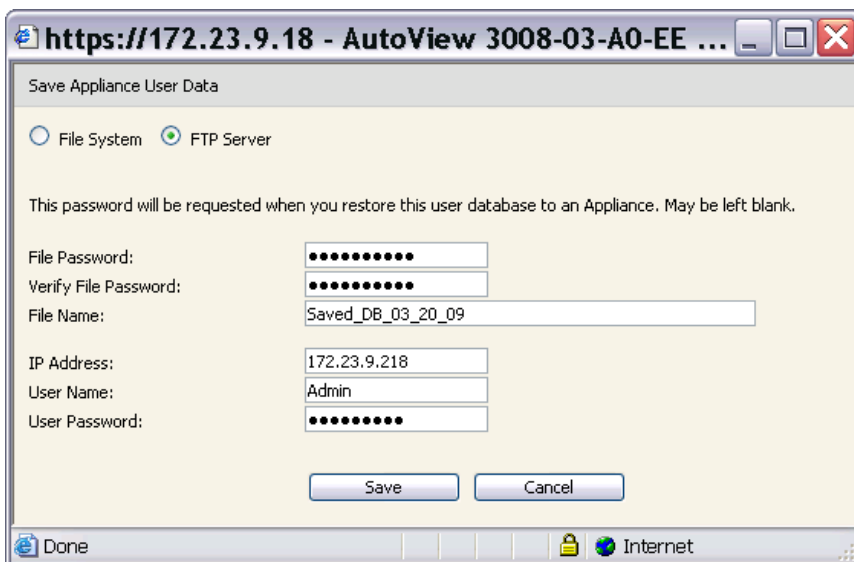
To read and save a configuration file from a AutoView switch:

1. Click the *Tools* tab in the OBWI.
2. Click the *Save Appliance Configuration* button.



The screenshot shows a web browser window titled "https://172.23.9.18 - AutoView 3008-03-A0-EE ...". The main content area is titled "Save Appliance Configuration". It features two radio buttons: "File System" (selected) and "FTP Server". Below this, a text block states: "This password will be requested when you restore this appliance configuration to an Appliance. May be left blank." There are two password input fields: "File Password:" and "Verify File Password:", both containing masked characters (dots). At the bottom, there are "Save" and "Cancel" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

Figure 4.14: Save Appliance Configuration Window (File System)



The screenshot shows a web browser window titled "https://172.23.9.18 - AutoView 3008-03-A0-EE ...". The main content area is titled "Save Appliance User Data". It features two radio buttons: "File System" and "FTP Server" (selected). Below this, a text block states: "This password will be requested when you restore this user database to an Appliance. May be left blank." There are several input fields: "File Password:" and "Verify File Password:" (both masked), "File Name:" (containing "Saved_DB_03_20_09"), "IP Address:" (containing "172.23.9.218"), "User Name:" (containing "Admin"), and "User Password:" (masked). At the bottom, there are "Save" and "Cancel" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

Figure 4.15: Save Appliance User Data Window (FTP Server)

3. (Optional) Enter and verify a password in the supplied fields. This password is requested when you restore this database to an AutoView switch. Click *Save*.

NOTE: You may leave the password field blank if you do not want to require a password for accessing the configuration file.

4. Navigate to a location to save the configuration file. The location appears in the Save To field.
5. Click *Save*.
6. When complete, a message appears prompting you to confirm the read completion. Click *OK* to return to the main window.

To restore a configuration file to an AutoView switch:

1. Click the *Tools* tab in the OBWI.
2. Click the *Restore Appliance User Data* button.
3. Select the location of the files to be restored.
4. Click *Restore*.
5. (Optional) Enter the password you created when the configuration database was saved and click OK.

NOTE: You may leave the password field blank if you did not create a password for the configuration file.

6. When complete, a message appears prompting you to confirm the write completion. Click *OK* to return to the main window.

Managing user databases

User database files contain all user accounts assigned in an AutoView switch. You can save your user account database file and use it to configure users on multiple AutoView switches by writing the user account file to the new switch.

NOTE: The user account file is encrypted and you will be prompted to create a password when you save the file. You will need to re-type this password when you write the file to a new unit.

To save a user database from a AutoView switch:

1. Click the *Tools* tab in the OBWI.
2. Click the *Save Appliance User Data* button.
3. Click *Browse* and navigate to a location to save the user database file. Click *Save*.
4. Enter and verify a password and click OK.
5. When complete, a message appears prompting you to confirm the read completion. Once confirmed, the Save Appliance User Database window will close and you are returned to the Tools window.

To restore a user database file to a AutoView switch:

1. Click the *Tools* tab in the OBWI.
2. Click the *Restore Appliance User Data* button.

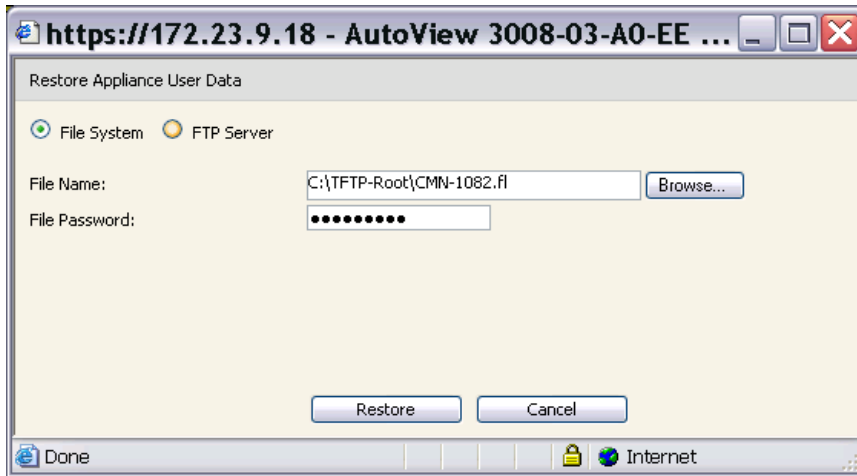


Figure 4.16: Restore Appliance User Data (File System) Window

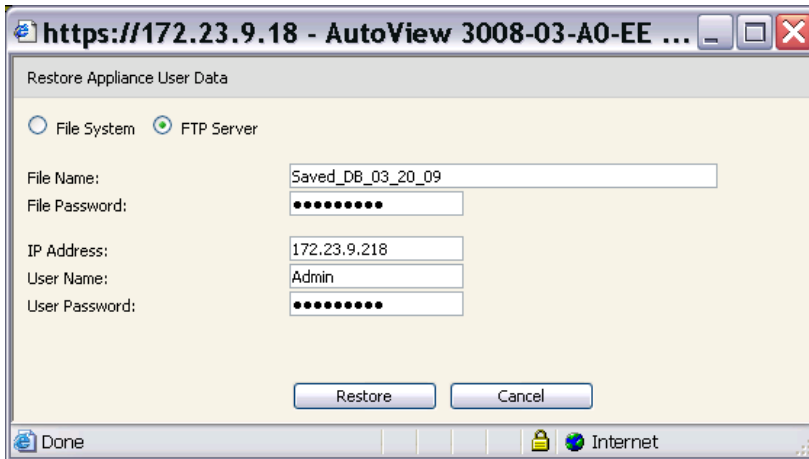


Figure 4.17: Restore Appliance User Data (FTP Server) Window

3. Click *Browse* and navigate to the location where you stored the saved user database file.
4. Click *Restore* and enter the password you created when the user database was saved. Click *OK*.
5. When complete, a message appears prompting you to confirm the write completion. Once confirmed, the Restore User Database File window will close and you are returned to the Tools window.

Configuring LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy and integrity.

If individual user accounts are stored on an LDAP-enabled directory service, such as Active Directory, you can use the directory service to authenticate users. The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the OBWI let you configure your authentication configuration parameters. The software sends the username, password and other information to the appliance, which then determines whether the user has permission to view or change configuration parameters for the appliance in the OBWI.

NOTE: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values may cause LDAP authentication server communication errors.

LDAP Overview parameters

On the Authentication page in the OBWI, you can configure the LDAP authentication priority and the parameters that define LDAP server connection information.

LDAP authentication priority

In the Authentication section of the OBWI, you can disable LDAP, or you can set the authentication priority by choosing whether local authentication or LDAP authentication should happen first.

To configure LDAP authentication priority parameters:

1. Select *Configure-Appliance-Authentication*.
2. Check the box next to Use LDAP Authentication. Then check the box for Use Local First or Use LDAP First to set the priority.
3. Click *Save*.

LDAP servers

The Server fields specify the host names or IP addresses of the primary and secondary LDAP servers. The secondary LDAP server is optional.

The Port fields specify the User Datagram Protocol (UDP) port numbers that communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP (LDAPS). The default Port ID is automatically entered by the software when an access type is specified.

The Access Type radio buttons specify how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords and other information sent between an appliance and LDAP server are sent as non-secure clear text. Use LDAPS for secure encrypted communication between an appliance and LDAP server.

To configure LDAP server parameters:

1. Select *Configure-Appliance-Authentication-Server*.
2. Identify the primary and secondary server address, port and access type in the appropriate fields or radio buttons.
3. Click *Save*.

LDAP Search parameters

On the LDAP Search page, you can configure the parameters used when searching for LDAP directory service users.

Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the LDAP Query page. The default values are `cn=Administrator`, `cn=Users`, `dc=yourDomainName` and `dc=com` and may be modified. For example, to define an administrator Distinguished Name (DN) for `test.view.com`, type **cn=Administrator, cn=Users, dc=test, dc=view, and dc=com**. Each Search DN value must be separated by a comma.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

Use the Search Base field to define a starting point from which LDAP searches begin. The modifiable default values are `dc=yourDomainName` and `dc=com`. For example, to define a search base for `test.com`, type **dc=test, dc=com**. Each Search Base value must be separated by a comma.

The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form `<name>=<% 1>`. The default value is `sAMAccountName=% 1`, which is correct for use with Active Directory. This field is required for LDAP searches.

To configure LDAP search parameters:

1. Select *Configure-Appliance-Authentication-Search*.
2. Enter the appropriate information in the Search DN, Search Password, Search Base and UID Mask fields.
3. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

LDAP Query parameters

On the LDAP Query page, you can configure the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators and users attempting to access the appliance itself. Query Mode (Server) is used to authenticate users that are attempting to access attached servers. Additionally,

each type of query has three modes that utilize certain types of information to determine whether or not an LDAP user has access to an appliance or connected target devices.

You can configure the following settings on the LDAP Query Page:

- The Query Mode (Appliance) parameters determine whether or not a user has access to the appliance.
- The Query Mode (Server) parameters determine whether a user has user access to servers connected to an appliance. The user does not have access to the appliance, unless granted by Query Mode (Appliance).
- The Group Container, Group Container Mask and Target Mask fields are only used for group query modes and are required when performing an appliance or device query.
- The Group Container field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects. Group objects are Active Directory objects that can contain users, computers, contacts and other groups. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object. For example, if the Notes property in the group objects is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query Page should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.
- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is “ou=%1”.
- The Target Mask field defines a search filter for the target device. The default value is “cn=%1”.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to User Attribute or Group Attribute. The default value is info.

To configure LDAP query parameters:

1. Select *Configure-Appliance-Authentication-Search*.
2. Select either *Basic*, *User Attribute* or *Group Attribute* for the Appliance Query Mode and the Server Query Mode.
3. Enter the appropriate information in the Group Container, Group Container Mask, Target Mask and Access Control Attribute fields.
4. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

Appliance and Server Query Modes

One of three modes can each be used for Query Mode (Appliance) and Query Mode (Server):

- **Basic** – A username and password query for the user is made to the directory service. If they are verified, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected server for Query Mode (Server).
- **User Attribute** – A username, password and Access Control Attribute query for the appliance user is made to the directory service. The Access Control Attribute is read from the user object (the user account) in Active Directory.

If the KVM Appliance Admin value is found, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Server).

If the KVM User Admin value is found, the user is given user administrator access to the appliance and attached target devices for Query Mode (Appliance), or to any selected server for Query Mode (Server). If the KVM User value is found, the user is given User access to the appliance for Query Mode (Appliance), or to any selected server for Query Mode (Server).

NOTE: If none of the three values are found, the user is given no access to the appliance and servers for Query Mode (Appliance) or to any selected target device for Query Mode (Server), unless the user has User Admin or Appliance Admin privileges to the appliance.

- **Group Attribute** – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance), or for a selected server when using Query Mode (Server). If a group is found containing the user and the appliance name, the user is given access to the appliance or attached target devices, depending on the group contents, when using Query Mode (Appliance). If a group is found containing the user and server IDs, the user is given access to the selected server connected to the appliance when using Query Mode (Server).

Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you may have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group may contain a member named Domestic, which is a group, etc.

Setting up Active Directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the user.

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create a computer object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview screen of the OBWI), or

identical to the attached target devices for querying target devices. The name must match exactly, including case.

5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview screen of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of uppercase and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.

NOTE: The factory default name in earlier versions contains a space that must be removed by editing the switching system name in the Appliance Overview screen of the OBWI.

6. Create one or more groups under the group container organizational unit.
7. Add the usernames and target device and appliance objects to the groups you created in step 5.
8. Specify the value of any attribute being used to implement the access control attribute. For example, if you are using info as the attribute in the Access Control Attribute field and using the Notes property in the group object to implement the access control attribute, the value of the Notes attribute in Active Directory may be set to one of the three available access levels (KVM User, KVM User Admin or KVM Appliance Admin) for the group object. The members of the group may then access the appliances and target devices at the specified access level.

NOTE: If none of the three values are found, the user is granted user level access to any appliance or target device listed in a group with the username.

Installing a Web Certificate

A web certificate allows you to access the OBWI without having to acknowledge the AutoView switch as a trusted web server each time you access it. Using the Install Web Certificate window, you can create a self-signed openssl certificate.

To install a web certificate:

1. Click the *Tools* tab in the OBWI.
2. Click the *Install Web Server Certificate* button.

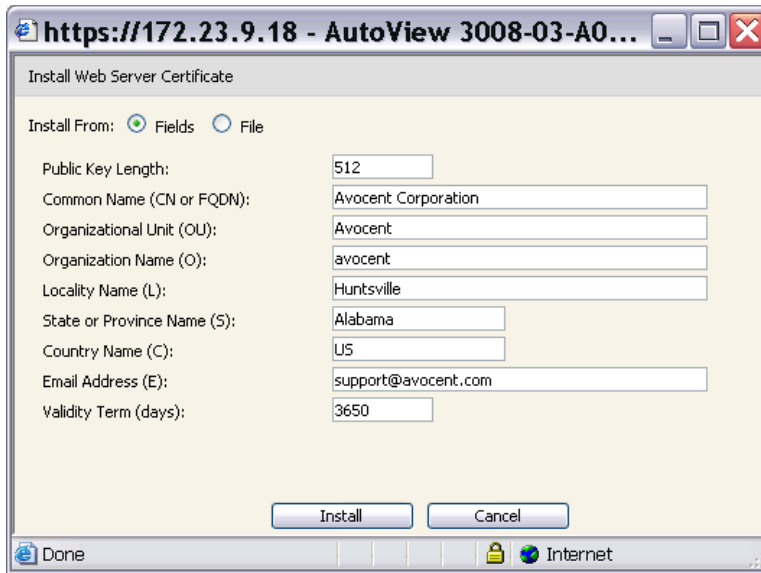


Figure 4.18: Install Web Server Certificate Window

3. Select the Fields radio button, and enter the following fields:
 - Public Key Length: the number of bits you want the certificate to be.
 - Common Name: your name. (Since this is your root certificate, use an appropriate name such as, "Company_Name Certificate Authority.")
 - Organizational Unit (optional): organization unit name (marketing, for example).
 - Organization Name: the exact legal unabbreviated name of your organization.
 - Locality Name: the city where your organization is located.
 - State or Province Name: the unabbreviated state or province where your organization is located.
 - Country Name: the two-letter ISO abbreviation for your country.
 - Email Address: the email address for the CA to contact.
 - Validity Term: number of days the certificate is valid.

-or-

Select to install from a file by clicking the File radio button, then download a company certificate file (*.pem).

NOTE: If importing a company certificate file, it may take up to 30 seconds for the OBWI to relaunch.

4. Select *Install*. Close the web browser, then relaunch the OBWI again for the same IP address.

5. When prompted, click to view the certificate and follow the instructions to import the certificate into the Root Certificate Authority folder. After the certificate is stored, the user should not see the certificate warning.

The Video Viewer

The Video Viewer Window

The Video Viewer is used to conduct a KVM session with the target devices attached to an AutoView 3008/3016 switch using the OBWI. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window containing both the local and the target device cursor. The Video Viewer window supports either a 3- or 5-button mouse.

The OBWI software uses a Java-based program to display the Video Viewer window. The OBWI automatically downloads and installs the Video Viewer the first time it is opened.

NOTE: Java Runtime Environment 1.6 or later is required.

NOTE: The AutoView 3008/3016 switch OBWI does not install the Java Runtime Environment (JRE). The JRE is available as a free download from <http://www.sun.com> for PC users and from <http://www.apple.com> for Mac users.

NOTE: The OBWI uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory:

- An 8-bit color setting on the client PC requires 1.4 MB of memory per Video Viewer window.
 - A 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB.
-

If the device you are attempting to access is currently being viewed by another user, you will be prompted to preempt the other user if your preemption level is equal to or greater than theirs. An appliance administrator can also disconnect an active user via the Active Session page.

Video Viewer Window Features

Figure 5.1 shows the Video Viewer window areas. Descriptions follow in Table 5.1.

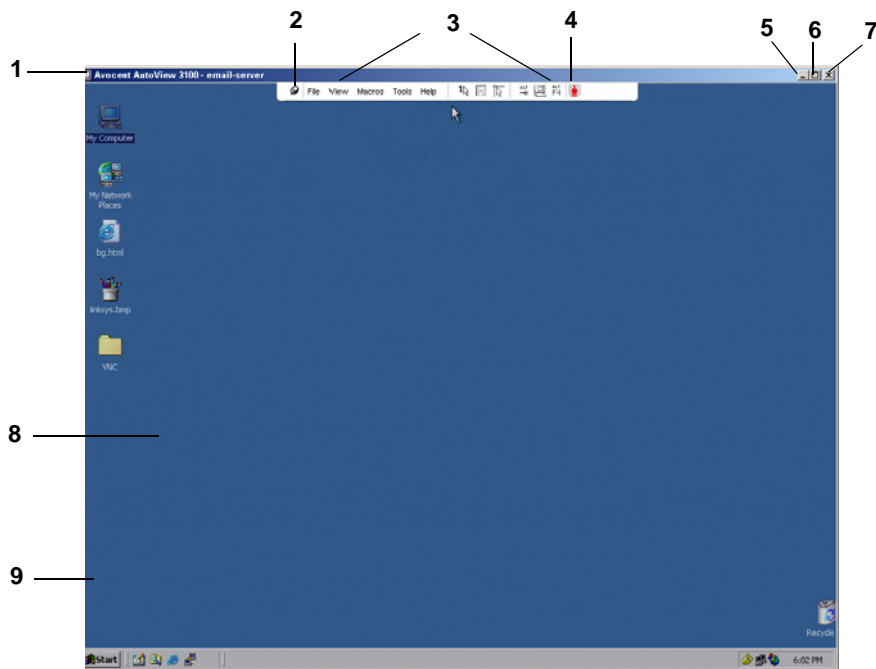


Figure 5.1: Video Viewer Window (Normal Window Mode)

Table 5.1: Descriptions for Figure 5.1

Number	Description
1	Title Bar: Displays the name of the server being viewed. When in Full Screen mode, the title bar disappears and the server name appears between the menu and toolbar.
2	Thumbtack: Locks the display of the menu and toolbar so that it is visible at all times.
3	Menu and toolbar: Enables you to access many of the features in the Video Viewer window. The menu and toolbar is in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons can be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. For more information, see the <i>Changing the toolbar</i> on page 69 and the <i>Using Macros</i> on page 78.
4	Macro buttons: Commonly used keyboard sequences that can be sent to the target device.
5	Minimize button: Minimizes the display of the Video Viewer window into the task bar at the bottom of the local computer.

Table 5.1: Descriptions for Figure 5.1 (Continued)

Number	Description
6	<p>Maximize button: Changes the window to Full Screen mode, which expands the accessed device desktop to fill the entire screen. Expanding the window causes the following to occur:</p> <ul style="list-style-type: none"> • The title bar disappears. • The server name appears between the menu and toolbar. • The Maximize button changes to a Normal Window Mode button and appears on the toolbar. Clicking the button toggles the Video Viewer window to Normal Window mode. • The Close button appears on the toolbar.
7	<p>Close button: Closes the Video Viewer window.</p> <p>NOTE: The Close button may not be present for all operating systems.</p>
8	<p>Accessed device desktop: Interacts with your device through this window.</p>
9	<p>Frame: Resizes the Video Viewer window by clicking and holding on the frame.</p>

Changing the toolbar

You can choose the amount of elapsed time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack).

To specify a toolbar hide time:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.
The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Use the arrow keys to specify the number of elapsed seconds prior to hiding the toolbar.
4. Click *OK* to save your changes and close the dialog box.

Setting the window size

NOTE: The *View - Scaling* command is not available if the Video Viewer window is in Full Screen mode.

When the OBWI is used for the first time, the Video Viewer windows display at a resolution of 1024 x 768 until the user changes the value.

The OBWI automatically adjusts the display if the window size changes during a session as long as autoscaling is enabled. If the target device resolution changes any time during a session, the display adjusts automatically.

To change the Video Viewer window resolution:

1. Select the *View - Scaling* command.

2. Click the desired resolution.

Adjusting the view

Using menus or task buttons in the Video Viewer window, you can do the following:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1024 x 768. If the desktop has a higher resolution, the following occurs:
 - The full-screen image is centered in the desktop, and the areas surrounding the Video Viewer window are black.
 - The menu and toolbar are locked so that they are visible at all times.
- Enable automatic, full or manual scaling of the session image:
 - With full scaling, the desktop window remains fixed and the device image scales to fit the window.
 - With automatic scaling, the desktop window is sized to match the resolution of the server being viewed.
 - With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Change the color depth of the session image.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor should align with the cursor on the remote device.

NOTE: If cursors drift out of alignment, turn off mouse acceleration in the attached device.

To refresh the screen:

Click the *Refresh Image* button in the Video Viewer window.

-or-

Select *View - Refresh* from the Video Viewer window menu.

The digitized video image is completely regenerated.

To enable or disable Full Screen mode:

To enable Full Screen mode, click the *Maximize* button.

-or-

Select *View - Full Screen* from the Video Viewer window menu.

The desktop window disappears and only the accessed device desktop is visible. The screen resizes up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

-or-

To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

To enable full or manual scaling:

To enable full scaling, select *View - Scaling* from the Video Viewer window menu. The device image scales automatically to the resolution of the server being viewed.

-or-

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu. Choose the dimension to scale the window. Available manual scaling sizes are as follows:

1024 x 768	768 x 576
960 x 720	704 x 528
896 x 672	640 x 480
832 x 624	

Adjusting color depth

The Dambrackas Video Compression® (DVC) algorithm enables users to adjust the number of viewable colors in a remote session window. You can choose to display more colors for the best fidelity or fewer colors to reduce the volume of data transferred on the network.

Video Viewer windows can be viewed using the Best Color Available (slower updates), Best Compression (fastest updates), a combination of Best Color and Best Compression or in Grayscale.

You can specify the color depths of individual ports and channels by selecting the *View - Color* command in a remote session window. These settings are saved individually per channel.

Additional video adjustment

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, users can fine-tune the video with the help of Avocent Technical Support by selecting the *Tools - Manual Video Adjust* command in the Video Viewer window menu or clicking the *Manual Video Adjust* button. This displays the Manual Video Adjust dialog box. Video adjustment is a per target setting.

Users can also verify the level of packets per second required to support a static screen by observing the packet rate located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only on the advice and with the help of Avocent Technical Support.

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu.
-or-
Click the *Manual Video Adjust* button.

The Manual Video Adjust dialog box appears. Figure 5.2 shows the dialog box, and descriptions follow in Table 5.2.

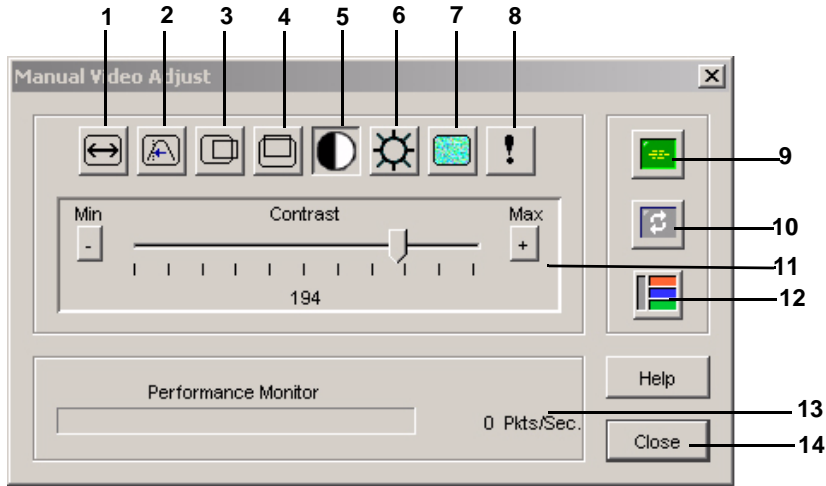


Figure 5.2: Manual Video Adjust Dialog Box

Table 5.2: Descriptions for Figure 5.2

Number	Description	Number	Description
1	Image Capture Width	8	Pixel Noise Threshold
2	Pixel Sampling/Fine Adjust	9	Automatic Video Adjustment
3	Image Capture Horizontal Position	10	Refresh Image
4	Image Capture Vertical Position	11	Adjustment bar
5	Contrast	12	Video Test Pattern
6	Brightness	13	Performance Monitor
7	Block Noise Threshold	14	Close button

2. Click the icon corresponding to the feature you wish to adjust.
3. Move the Contrast slider bar and then fine-tune the setting by clicking the *Min* (-) or *Max* (+) buttons to adjust the parameter for each icon pressed. The adjustments display immediately in the Video Viewer window.
4. When finished, click *Close* to exit the Manual Video Adjust dialog box.

Target video settings

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized and are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Contrast and brightness

If the image in the Video Viewer window is too dark or too light, select *Tools - Automatic Video Adjust* or click the *Automatic Video Adjust* button. This command is also available in the Video Adjustments dialog box. In most cases, this corrects video issues.

When clicking *Auto Adjust* several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually can help. Increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up, which is indicated by little dots changing in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and can improve cursor tracking.

You can modify Noise Threshold and Priority Threshold values if you are using standard video compression. You can also modify Block Noise Threshold and Pixel Noise Threshold values. You can restore default threshold values by clicking *Auto Adjust Video*.

Block Noise Threshold and Pixel Noise Threshold

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed.

- The Block Noise Threshold sets the minimum color change that occurs in a single video block. Increasing the value reduces the network bandwidth. Decreasing the value makes the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value reduces the number of low-contrast artifacts, but increases network bandwidth.

See *Adjusting the view* on page 70 for information about changing the color depth.

Automatic video adjustment

In most cases, you do not need to alter the Video Settings from the default. The system automatically adjusts and uses the optimal video parameters. The AutoView 3008/3016 switch OBWI performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You can easily adjust your video parameters to ideal settings by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box.

NOTE: You can also select *Tools - Automatic Video Adjust* from the Video Viewer window menu or click the *Automatic Video Adjust* toolbar icon to automatically adjust the video.

Refresh Image

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box completely regenerates the digitized video image.

NOTE: You can also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Video Test Pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box toggles a display of a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Adjusting mouse options

The Video Viewer window mouse options affect cursor type, Cursor mode, scaling, alignment and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

NOTE: If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor type

The Video Viewer window offers five appearance choices for the local mouse cursor. You can also choose no cursor or the default cursor.

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window turns off and only the target device mouse pointer is visible. The only mouse movements that appear are those of the target device remote cursor. Use Single Cursor mode when there is no need for a local cursor. Figure 5.3 shows both the Remote Cursor and the Local Cursor displayed in the Video Viewer window.

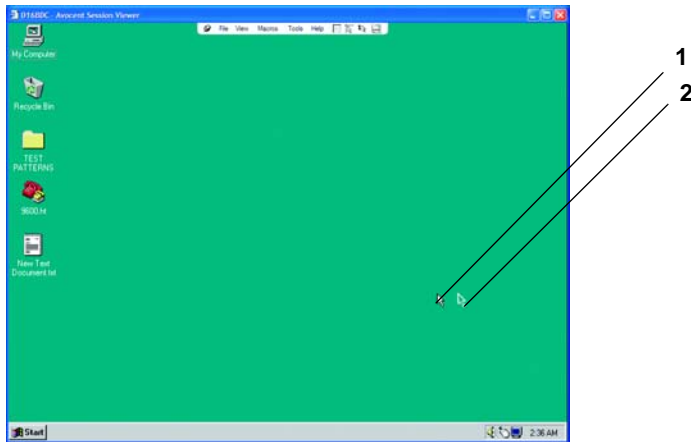


Figure 5.3: Video Viewer Window with Local and Remote Cursors Displayed

Table 5.3: Descriptions for Figure 5.3

Number	Description
1	Remote Cursor
2	Local Cursor

The Cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You can define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the client, you should avoid using those keys to restore the mouse pointer.

To enter Single Cursor mode:

Select *Tools - Single Cursor Mode* from the Video Viewer window menu.

-or-

Click the *Single Cursor Mode* button.

The local cursor does not appear and all movements are relative to the target device.

To select a key for exiting Single Cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu.

-or-

Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK* to save settings.

When you enable Single Cursor mode, you can press the specified key to return to Regular Desktop mode.

To exit Single Cursor mode:

Press the key on the keyboard that is identified in the title bar.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK* to save settings.

Mouse scaling

Some earlier versions of Linux did not support adjustable mouse accelerations. For installations that must support these earlier versions, you can choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are Default (1:1), High (2:1) or Low (1:2):

- In a 1:1 scaling ratio, every mouse movement on the desktop window sends an equivalent mouse movement to the server.
- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.
- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.
-or-
To set custom scaling:

- a. Click the *Custom* radio button to enable the X and Y fields.
- b. Type a scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input range is 0.25-3.00.

Vendor-specific video settings

Video settings vary significantly among manufacturers. Avocent maintains an online database of optimized video settings for various video cards, particularly Sun-specific ones. This information can be obtained from Avocent's online knowledge base or by calling Avocent technical support.

Mouse alignment and synchronization

Because the AutoView 3008/3016 switch OBWI cannot get constant feedback from the mouse, there are times when the mouse on the AutoView 3008/3016 switch may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you can align the mouse to re-establish proper tracking.

Alignment causes the local cursor to align with the remote server's cursor. Resetting causes a simulation of a mouse and keyboard reconnect as if you had disconnected and reconnected them.

To realign the mouse:

Click the *Align Local Cursor* button in the Video Viewer window toolbar.

Using Keyboard Pass-through

Keystrokes that a user enters when using a Video Viewer window may be interpreted in two ways, depending on the Screen mode of the Video Viewer window.

- If a Video Viewer window is in Full Screen mode, all keystrokes and keyboard combinations except **Ctrl-Alt-Del** are sent to the remote server being viewed.
- If a Video Viewer window is in Regular Desktop mode, Keyboard Pass-through mode can be used to control whether the remote server or local computer recognizes certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the Session Options dialog box. When enabled, keyboard pass-through sends all keystrokes and keystroke combinations except **Ctrl-Alt-Del** to the remote server being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The **Ctrl-Alt-Delete** keyboard combination can be sent only to a remote server by using a macro.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote server regardless of the Screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.
The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK* to save setting.

Using Macros

The AutoView 3008/3016 switch OBWI comes pre-configured with macros for the Windows and the Sun platforms.

To send a macro:

Select *Macros - <desired macro>* from the Video Viewer window menu.

-or-

Select the desired macro from the buttons available on the Video Viewer menu.

Saving the View

You can save the display of a Video Viewer either to a file or to the clipboard for pasting into a word processor or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu.
-or-
Click the *Capture to File* button.
The Save As dialog box appears.
2. Enter a filename and choose a location to save the file.
3. Click *Save* to save the display to a file.

To capture the Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the Video Viewer window menu.

-or-

Click the *Capture to Clipboard* button.

The image data is saved to the clipboard.

Closing a Video Viewer Window Session

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

Terminal Operations

The Console Menu

Each AutoView 3008/3016 switch may also be configured at the appliance level through the Console menu interface accessed through the 10101 port. All terminal commands are accessed through a terminal or PC running terminal emulation software.

To connect a terminal to the AutoView 3008/3016 switch:

1. Using a DB9 M/F serial cable, connect a terminal or a PC that is running terminal emulation software (such as HyperTerminal®) to the 10101 port on the back panel of the AutoView 3008/3016 switch. The terminal settings are 9600 bits per second (bps), 8 bits, 1 stop bit, no parity and no flow control.
2. Turn on the AutoView 3008/3016 switch and each target device. When the AutoView 3008/3016 switch completes initialization, the Console menu will display the following message:
Press any key to continue.

Network Configuration

To configure network settings using the Console menu:

1. When you turn on your AutoView 3008/3016 switch, the switch initializes for approximately one minute. After it completes initialization, press any key on the terminal or on the PC running the terminal emulation software to access the Console menu interface.

NOTE: The terminal may be connected at any time, even when the switch is already turned on.

2. Once the Console Main menu displays, type the number corresponding to Network Configuration and press **Enter**.
3. Type **1** and press **Enter** to set your network speed. For best performance, set the AutoView 3008/3016 switch at the same speed as the Ethernet switch to which it is attached. After you press **Enter**, you will be returned to the Console Network Configuration menu.
4. Type **2** and press **Enter** to specify whether you are using a static or Dynamic Host Configuration Protocol (DHCP) address.

A static IP configuration may be used to provide a user-defined IP address, netmask or prefix length, and default gateway for the AutoView 3008/3016 switch.

DHCP is a protocol that automates the configuration of TCP/IP-enabled computers. When DHCP is selected, the IP address, netmask or prefix length, and default gateway settings are automatically assigned to the AutoView 3008/3016 switch and may not be modified by an AutoView 3008/3016 switch user.

If you are using the DHCP option, please configure your DHCP server to provide an IP address to the AutoView 3008/3016 switch and then skip to step 6.

5. Select the remaining options from the Network Configuration menu to finish the configuration of your AutoView 3008/3016 switch with an IP address, netmask or prefix length and default gateway.
6. Type **0** (zero) and press **Enter** to return to the Console Main menu.

Other Console Main Menu Options

Besides the Network Configuration option, the Console Main menu of the AutoView 3008/3016 switch features the following menu items: Firmware Management, Enable Debug Messages, Set/Change Password, Restore Factory Defaults, Reset Appliance, Set Web Interface Ports, Input Web Server Certificate and Exit. Each menu item is discussed in this section.

Firmware Management

This menu contains the Flash Download selection. For more information, see *Flash Upgrades* section on page 85.

Enable Debug Messages

This menu option turns on console status messages. Because this can significantly reduce performance, you should only enable debug messages when instructed to do so by Avocent Technical Support. When you are finished viewing the messages, press any key to exit this mode.

Set/Change Password

This menu option allows enabling and disabling of serial port security, which locks the serial port with a user-defined password.

Restore Factory Defaults

This menu option will restore all switch options to the default settings.

Reset Appliance

This menu option allows you to execute a soft reset of the AutoView 3008/3016 switch.

Set Web Interface Ports

Currently, the appliance and client software are using ports 80 and 443 for HTTP and HTTPS port numbers respectively. Now the user will have the ability to modify or specify alternate ports.

Input Web Server Certificate

This menu option allows the user to utilize the User Defined Web Certificate, Import or Export Web Certificates options.

Exit

This menu selection will return you to the ready prompt. If the Console menu interface password is enabled, you must exit the Console Main menu so that the next user will be prompted with the Username and Password login screen.

APPENDICES

Appendix A: Flash Upgrades

The AutoView 3008/3016 switch Flash upgrade feature allows you to update your appliance with the latest firmware available. This update can be performed using a Trivial File Transfer Protocol (TFTP) server, File Transfer Protocol (FTP) or using the OBWI.

After the Flash memory is reprogrammed with the upgrade, the AutoView 3008/3016 switch performs a soft reset, which terminates all IQ module sessions. A target device experiencing an IQ module firmware update may not display, or may display as disconnected. The target device will appear normally when the Flash update is completed.



NOTE: During an IQ module upgrade, the IQ module status indicator in the OSCAR interface Main dialog box is yellow.

CAUTION: Disconnecting an IQ module during a firmware update or cycling power to the target device will render the module inoperable and require the IQ module to be returned to the factory for repair.

Using the Console menu interface

To upgrade the AutoView 3008/3016 switch firmware using the Console menu interface:

NOTE: If you do not have a TFTP server, you can find several shareware and freeware programs on the Internet that you can download and install.

1. Visit <http://www.avocent.com/support> and download the latest Flash firmware from Avocent.
2. Save the Flash upgrade file to the appropriate directory on the TFTP or FTP server.
3. Use the DB9 M/F serial cable to connect a terminal or PC running terminal emulation software (such as HyperTerminal) to the SETUP, CONSOLE or 10101 port on the back panel of the AutoView 3008/3016 switch. The terminal should be set to 9600 bps, 8 bits, 1 stop bit, no parity and no flow control.
4. If the AutoView 3008/3016 switch is not on, turn it on now. After approximately one minute, press any key to access the Console Main menu.
5. Select the *Firmware Management* option from the Console Main menu.

NOTE: The current version of your firmware will be displayed on the Firmware Management menu.

6. Type **1** and press **Enter** to access Flash Download.
7. Type the IP address of your TFTP server and press **Enter**.
8. Enter the name of the file that you downloaded from the Avocent web site.
9. Confirm the TFTP download by typing a **y** or **yes** and pressing **Enter**.

10. The AutoView 3008/3016 switch will begin the Flash upgrade process. On-screen indicators will display the upgrade progress. When the upload is complete, the AutoView 3008/3016 switch will reset and upgrade the internal subsystems.
11. The Console menu will display the following message: *Press any key to continue.*

Recovering from a failed Flash upgrade

NOTE: If the green power LED on the front and back panel of the switch blinks continuously, the switch is in recovery mode.

To recover from a failed Flash upgrade:

1. Visit <http://www.avocent.com/support> and download the latest Flash firmware from Avocent.
2. Save the Flash upgrade file to the appropriate directory on the TFTP server.
3. Set up the TFTP server with the server IP address 10.0.0.20.
4. Rename the downloaded file the appropriate name from the following list and place it into the TFTP root directory of the TFTP server:
 - CMN-1082.fl
5. Attach a cross-over CAT 5 cable to the AutoView 3008/3016 switch for this process instead of a standard CAT 5 cable.
6. If the AutoView 3008/3016 switch is not on, turn it on now.
7. The recovery process should start automatically.

Appendix B: Using Serial IQ Modules

The serial IQ module is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the AutoView 3008/3016 switch local port or the OBWI. The actual serial data is not accessed, but is merely displayed. All serial data coming from the target device is displayed in a VT100 window, placed into a video buffer and sent to the AutoView 3008/3016 switch as though it came from a VGA target. Likewise, keystrokes entered on a keyboard are sent to the attached device as though they were typed on a VT100 terminal.

Serial IQ module modes

The following modes can be accessed from the serial IQ module:

- **On-Line:** This mode enables you to send and receive serial data.
- **Configuration:** This mode enables you to specify AutoView 3008/3016 switch communication parameters, the appearance of the Terminal Applications menu and key combinations for specific actions and macros.
- **History:** This mode enables you to review serial data.

Configuring the serial IQ module

NOTE: The serial IQ module is a DCE device and only supports VT100 terminal emulation.

Pressing **Ctrl-F8** will activate the Configuration screen of the IQ module's Terminal Applications menu, which enables you to configure your serial IQ module.

NOTE: When any Terminal Applications menu is active, pressing **Enter** saves changes and returns you to the previous screen. Pressing **Escape** returns you to the previous screen without saving changes.

Within the Terminal Applications menu's Configuration screen, you can modify the following options:

- **Baud Rate:** This option allows you to specify the serial port communications speed. Available options are 300, 1200, 2400, 9600, 19,200, 34,800, 57,600 or 115,200 bps. The default value is 9600.
- **Parity:** This option allows you to specify the serial port's communications parity. Available options are EVEN, ODD or NONE. The default value is NONE.
- **Flow Control:** This option allows you to specify the type of serial flow control. Available options are NONE, XOn/XOff (software) and RTS/CTS (hardware). The default value is NONE. If you select a bps rate of 115,200, the only available flow control is RTS/CTS (hardware).
- **DSR CD Mode:** This option allows you to control how the DSR and CD lines operate. Available options are Always on and Toggle. When in Toggle mode, DSR and CD lines are turned off for one-half second and then turned on each time a module is selected or deselected. The default value is Always on.

- **Enter Sends:** This option enables you to specify the keys that are transmitted when **Enter** is pressed. Available options are <CR> (Enter), which moves the cursor to the left side of the screen, or <CR><LF> (Enter-Linefeed), which moves the cursor to the left side of the screen and down one line.
- **Received:** This option enables you to specify how the module translates a received **Enter** character. Available options are <CR> (Enter) or <CR><LF> (Enter-Linefeed).
- **Background:** This option changes the screen's background color. The currently-selected color displays in the option line as it is changed. Available colors are Black, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Black. This value cannot be identical to the Normal Text or Bold Text value.
- **Normal Text:** This option changes the screen's normal text color. The currently-selected color displays in the option line as it is changed. Available colors are Grey, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Grey. This value cannot be identical to the Bold Text or Background value.
- **Bold Text:** This option changes the screen's bold text color. The currently-selected color displays in the option line as it is changed. Available colors are White, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon, Brown and Light Grey. The default color is White. This value cannot be identical to the Normal Text or Background value.
- **Screen Size:** This option allows you to specify the screen's text width size. Available values are widths of 80 columns or 132 columns. The length for both widths is 26 lines.

The following options for the Terminal Application menu's Configuration screen enable you to define the function keys that will perform a selected action. To specify a new function key, press and hold the **Ctrl** key, then press the function key that you want to associate with the action. For example, if you want to change the Configuration (Config) Key Sequences option from <CTRL-F8> to <CTRL-F7>, press and hold the **Ctrl** key and then press **F7**.

- **Config Key Sequences:** This option allows you to define the key combination that makes the Terminal Application menu's Configuration screen appear. The default key sequence is **Ctrl-F8**.
- **On-Line Key Sequence:** This option allows you to define the key sequence that displays the On-Line mode. The default key sequence is **Ctrl-F10**.
- **Help Key Sequence:** This option allows you to define the key combination that displays the Help System screen. The default key sequence is **Ctrl-F1**.
- **History Key Sequence:** This option allows you to define the key combination that enables History mode. The default key sequence is **Ctrl-F9**.
- **Clear History Key Sequence:** This option allows you to define the key combination that clears the history buffer while in History mode. The default key sequence is **Ctrl-F11**.
- **Break Key Sequence:** This option allows you to configure the key combination that generates a break condition. The default key sequence is **Alt-B**.

To configure a serial IQ module:

1. Press **Ctrl-F8**. The Configuration Screen will appear.
2. Select a parameter to change. You can navigate the Configuration Screen using the **Up Arrow** and **Down Arrow** keys.
3. Modify the selected value using the **Left Arrow** and **Right Arrow** keys.
4. Repeat steps 2 and 3 to modify additional values.
5. Press **Enter** to save your changes and exit the Configuration Screen.
-or-
Press **Escape** to exit the Configuration Screen without saving the changes.

Creating a serial IQ module macro

Pressing the **Page Down** key when the Terminal Applications menu's Configuration screen is displayed will provide access to the Macro Configuration screen. The serial IQ module can be configured with up to 10 macros. Each macro can be up to 128 characters in length.

To create a macro:

1. Select the serial IQ module you wish to configure and press **Ctrl-F8** to activate the Terminal Applications menu's Configuration screen.
2. When the Terminal Applications menu appears, press **Page Down** to view the Macro Configuration screen. The Macro Configuration screen shows the 10 available macros and the associated key sequences, if any, for each.
3. Using the **Up Arrow** and **Down Arrow** keys, scroll to an available macro number and highlight the listed keystroke sequence. Type the new macro keystroke sequence over the default. Any combination of **Ctrl** or **Alt** and a single key may be used. When you have finished entering the keystroke sequence that will activate the new macro, press the **Down Arrow** key.
4. On the line below the macro keystroke sequence you just entered, type the keystroke sequence that you wish the macro to perform.
5. Repeat steps 3 and 4 to configure additional macros.
6. When finished, press **Enter** to return to the previous screen.

Using History mode

History mode allows you to examine the contents of the history buffer, which contains the events that have occurred.

The serial IQ module maintains a buffer containing 240 lines minimum, or 10 screens, of output. When the history buffer is full, it will add new lines at the bottom of the buffer and delete the oldest lines at the top of the buffer.

NOTE: The Config Key Sequence, On-Line Key Sequence and Clear History Key Sequence used in the following procedure are the default values. These key combinations can be changed using the Terminal Applications menu.

To use History mode:

1. Press **Ctrl-F9**. The mode will display as History.
2. Press one of the following key combinations to perform the indicated action:
 - **Home**: Move to the top of the buffer.
 - **End**: Move to the bottom of the buffer.
 - **Page Up**: Move up one buffer page.
 - **Page Down**: Move down one buffer page.
 - **Up Arrow**: Move up one buffer line.
 - **Down Arrow**: Move down one buffer line.
 - **Ctrl-F8**: Enters Configuration mode. The Configuration screen will appear.
 - **Ctrl-F9**: While in Configuration mode, returns to the previous screen with History mode enabled.
 - **Ctrl-F10**: While in Configuration mode, returns to the previous screen with On-Line mode enabled.
 - **Ctrl-F11**: Clears the history buffer. If you choose this option, a warning screen will appear. Press **Enter** to delete the history buffer or **Escape** to cancel the action. The previous screen will reappear.
3. When finished, press **Ctrl-F10** to exit History mode and return to On-Line mode.

Serial IQ module pinouts

Table B.1 lists the pinouts for the serial IQ module.

Table B.1: Serial IQ Module Pinouts

DB9-F Pin	Host Signal Name Description	Signal Flow	SRL Signal Name Description
1	DCD - Data Carrier Detect	Out of SRL	DTR - Data Terminal Ready
2	RXD - Receive Data	Out of SRL	TXD - Transmit Data
3	TXD - Transmit Data	In to SRL	RXD - Receive Data
4	DTR - Data Terminal Ready	In to SRL	DSR - Data Set Ready
5	GND - Signal Ground	N/A	GND - Signal Ground
6	DSR - Data Set Ready	Out of SRL	DTR - Data Terminal Ready
7	RTS - Request to Send	In to SRL	CTS - Clear to Send
8	CTS - Clear to Send	Out of SRL	RTS - Request to Send
9	N/C - Not Connected	N/A	N/C - Not Connected

Appendix C: UTP Cabling

This appendix discusses various aspects of connection media. The performance of an AutoView 3008/3016 switching system depends on high quality connections. Poor quality or poorly installed or maintained cabling can diminish AutoView 3008/3016 switching system performance. AutoView 3008/3016 switching systems utilize UTP cabling.

NOTE: This appendix is for information purposes only. Please consult with your local code officials and/or cabling consultants prior to any installation.

UTP copper cabling

The following are basic definitions for the three types of UTP cabling that the AutoView 3008/3016 switch supports:

- UTP (4-pair) high performance cable consists of twisted pair conductors, used primarily for data transmission. The twisting of the pairs gives this cable some immunity from the infiltration of unwanted interference. UTP cable is generally used for networks running at 10 or 100 Mbps.
- CAT 5E (enhanced) cable has the same characteristics as CAT 5, but is manufactured to somewhat more stringent standards.
- CAT 6 cable is manufactured to tighter requirements than CAT 5E cable. CAT 6 has higher measured frequency ranges and significantly better performance requirements than CAT 5E cable at the same frequencies.

Wiring standards

There are two supported wiring standards for 8-conductor (4-pair) RJ-45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to installations utilizing CAT 5, 5E and 6 cable specifications. The AutoView 3008/3016 switching system supports either of these wiring standards. Table C.1 describes the standards for each pin.

Table C.1: UTP Wiring Standards

Pin	EIA/TIA 568A	EIA/TIA 568B
1	white/green	white/orange
2	green	orange
3	white/orange	white/green
4	blue	blue
5	white/blue	white/blue
6	orange	green
7	white/brown	white/brown

Table C.1: UTP Wiring Standards (Continued)

Pin	EIA/TIA 568A	EIA/TIA 568B
8	brown	brown

Cabling installation, maintenance and safety tips

The following is a list of important safety considerations that should be reviewed prior to installing or maintaining your cables:

- Keep all UTP runs to a maximum of 100 feet each.
- Maintain the twists of the pairs all the way to the point of termination, or no more than one-half inch untwisted. Do not skin off more than one inch of jacket while terminating.
- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.
- Dress the cables neatly with cable ties, using low to moderate pressure. Do not over tighten the ties.
- Cross-connect cables where necessary, using rated punch blocks, patch panels and components. Do not splice or bridge the cable at any point.
- Keep the UTP cable as far away as possible from potential sources of EMI, such as electrical cables, transformers and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.
- Always test every installed segment with a cable tester. "Toning" alone is not an acceptable test.
- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.
- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 15 feet at the patch panel side.
- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Don't mix 568A and 568B wiring in the same installation.
- Always obey all local and national fire and building codes. Be sure to firestop all the cables that penetrate a firewall. Use plenum rated cable where it is required.

Appendix D: Technical Specifications

Table D.1: AutoView 3008/3016 Switch Product Specifications

Server Ports	
Number	16 - AutoView 3016 switch 8 - AutoView 3008 switch
Type	PS/2, Sun, USB and Serial
Connectors	8-pin modular
Sync Types	Separate horizontal and vertical
Plug and Play	DDC2B
Video Resolution	640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz
Supported Cabling	4-pair UTP CAT 5 or CAT 6, 150 feet (45 meters) maximum length
Dimensions	
Form Factor	1-U rack mountable
Height x Width x Depth	1.72 x 17.00 x 6.5 in (4.37 x 43.18 x 16.51 cm)
Weight (without cables)	4.2 lbs (1.9 kg)
SETUP Port	
Number	1
Type	RS-232 serial
Connector	DB9 male

Table D.1: AutoView 3008/3016 Switch Product Specifications (Continued)

Network Connection	
Number	1
Type	10/100 Ethernet
Connector	8-pin modular
Local Port	
Number	1
Type	PS/2, USB and VGA
USB Device Port	
Number	2
Type	USB 1.1
Power Supply	
Type	Internal
Power	8.5 W
Heat Dissipation	29 BTU/hr
AC-input Range	100 - 240 VAC
AC Frequency	50 - 60 Hz autosensing
AC-input Current Rating	0.5 A
AC-input Power (maximum)	15 W
AC-input Cable	18 AWG three-wire cable, with a three-lead IEC-320; receptacle on the power supply end and a country-dependent plug on the power resource end
Ambient Atmospheric Condition Ratings	
Temperature	32 to 104 degrees Fahrenheit (0 to 40 degrees Celsius) operating; -4 to 158 degrees Fahrenheit (-20 to 70 degrees Celsius) nonoperating
Humidity	10 - 95% noncondensing
	UL, FCC, cUL, ICES-003, CE, VCCI, MIC, C-Tick, GOST
Safety and EMC Standards Approvals and Markings	Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

Appendix E: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on a PS/2 keyboard. To enable Sun Advanced Key Emulation mode and use these keys, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key. The *Scroll Lock* LED blinks. Use the indicated keys in Table E.1 as you would use the advanced keys on a Sun keyboard.

Table E.1: Sun Key Emulation

Sun Key (US)	PS/2 Key to Enable Sun Key Emulation
Compose	Application ⁽¹⁾
Compose	keypad
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left) ⁽²⁾	F12
Command (left) ⁽²⁾	Win (GUI) left ⁽¹⁾
Command (right) ⁽²⁾	Win (GUI) right ⁽¹⁾

(1)Windows 95 104-key keyboard.

(2)The Command key is the Sun Meta (diamond) key.

For example: For **Stop + A**, press and hold **Ctrl+Shift+Alt** and press Scroll Lock, then **F1 + A**.

These key combinations will work with the serial USB IQ module (if your Sun system comes with a USB port) as well as the Sun VSN and WSN IQ modules. With the exception of **F12**, these key combinations are not recognized by Microsoft Windows. Using **F12** performs a Windows key press.

When finished, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key to toggle Sun Advanced Key Emulation mode off.

Special considerations for Japanese Sun USB and Korean Sun USB keyboards (USB IQ modules only)

Japanese Sun USB and Korean Sun USB keyboards assign usage IDs for certain keys that differ from standard USB usage IDs. If USB IQ modules are attached to your Sun servers, the Han/Zen and Katakana/Hiragana keys on Japanese Sun USB keyboards and Hangul and Hanja keys on Korean Sun USB keyboards must be accessed using alternate keystrokes.

Due to these keyboard-specific differences, keyboard mapping inconsistencies may be encountered when switching between target devices using Sun VSN and WSN IQ modules and target devices using USB IQ modules. These keys function normally if your Sun servers are attached to the AutoView 3008/3016 switch using a VSN or WSN IQ module.

Table E.2 lists the keyboard mapping that will take place when a USB IQ module is used in this setting.

Table E.2: PS/2-to-USB Keyboard Mappings

PS/2 Keyboard	USB Usage ID	Sun USB Keyboard	Korean Sun USB Keyboard	Japanese Sun USB Keyboard
Right-Alt	0xE6	AltGraph	Hangul	Katakana/Hiragana
Windows Application	0x65	Compose	Hanja	Compose
Hangul	0x90	N/A	N/A	N/A
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35	~	~	N/A

Appendix F: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Visit www.avocent.com/support and use one of the following resources:
3. Search the knowledge base or use the online service request.
-or-
Select *Technical Support Contacts* to find the Avocent Technical Support location nearest you.



Avocent[®]

The Power of Being There[®]

For Technical Support:
www.avocent.com/support